# A Survey on Key Management Strategies for Different Applications of Wireless Sensor Networks

Syed Muhammad Khaliq-ur-Rahman Raazi and Sungyoung Lee[†]
Department of Computer Engineering
Kyung Hee University (Global Campus), Korea
{raazi,sylee}@oslab.khu.ac.kr

Received 10 November 2009; Revised 2 February 2010; Accepted 24 February 2010

Wireless Sensor Networks (WSN) have proved to be useful in applications that involve monitoring of real-time data. There is a wide variety of monitoring applications that can employ Wireless Sensor Network. Characteristics of a WSN, such as topology and scale, depend upon the application, for which it is employed. Security requirements in WSN vary according to the application dependent network characteristics and the characteristics of an application itself. Key management is the most important aspect of security as some other security modules depend on it. We discuss application dependent variations in WSN, corresponding changes in the security requirements of WSN and the applicability of existing key management solutions in each scenario.

Categories and Subject Descriptors: Information Security in Wireless Sensor Networks [**Key Management**]:

General Terms: Wireless Sensor Networks, Security, Key Management, Application Dependent Sensor Networks

Additional Key Words and Phrases: Small Scale Sensor Networks, Large Scale Sensor Networks, Application Dependent Network Topology, Wireless Body Area Networks}

## 1. INTRODUCTION

In a typical WSN scenario, a group of sensor nodes are used to monitor certain phenomena in their surrounding environment. These phenomena can be anything that a sensor node can sense and quantify. Sensor nodes then relay the quantified readings to a central server through a network of sensor nodes [Tilak et al. 2002]. The central server gathers all the readings and then processes them according to the application, for which the WSN was installed. For example, in soil moisture application

[†]: corresponding author

Copyright(c)2010 by The Korean Institute of Information Scientists and Engineers (KIISE). Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Permission to post author-prepared versions of the work on author's personal web pages or on the noncommercial servers of their employer is granted without fee provided that the KIISE citation and notice of the copyright are included. Copyrights for components of this work owned by authors other than KIISE must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists, requires an explicit prior permission and/or a fee. Request permission to republish from: JCSE Editorial Office, KIISE. FAX +82 2 521 1352 or email office@kiise.org. The Office must receive a signed hard copy of the Copyright form.

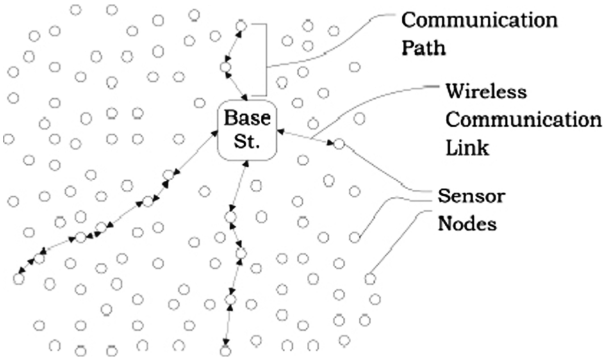


Figure 1. Wireless Sensor Network for Soil Moisture Application. Base station is the central server in this case. Communication link between two sensor nodes can be formed if they lie within the communication range of each other.

sensor nodes sense soil moisture and relay their readings to a central server through other sensor nodes, if they cannot do it directly. Figure 1 shows an example of wireless sensor network used for monitoring soil moisture.

Apart from data processing, applications also have an effect on the characteristics of the WSN such as the number of nodes, their deployment strategy and their network topology. For example, a WSN deployed for military applications should have a large number of nodes deployed in a hostile environment. On the other hand, a WSN deployed for healthcare applications is very small in number and deployed indoors. These are two application scenarios that are in extreme contrast with each other. In fact there are many different application scenarios of WSN. For example, some networks are so large and dense that they require intermediate nodes to do in-network processing [Akyildiz et al. 2002].

In many applications of WSN, like military surveillance, security is the most important part. In other applications, it is very important to conceal secret information from both active and passive adversaries. An adversary can also try to act like an authorized node in order to extract important information from a legitimate node. Even if an adversary cannot get to know the confidential information, it can try to disrupt communication or tamper with the messages, so that the WSN cannot perform the task, for which it was deployed.

Although security is an important part of a WSN, it also incurs overhead. Apart from depleting energy of sensor nodes and incurring communication and computation overhead, security schemes may require additional memory. Security was an important area of research even before the introduction of wireless sensor networks. Reliable security mechanisms like Diffie-Hellman key exchange algorithm [Diffie and Hellman 1976], RSA [Rivest et al. 1978], TLS [Deirks and Allen 1999] and Kerberos [Kohl and Neuman 1993] existed even before the introduction of WSN. However, these protocols did not consider resource constraints as an important issue.

Along with minimizing the resource usage, confidentiality, integrity, availability and authenticity should be maintained in all types of WSN. In order to compromise confidentiality, integrity, availability and authentication of a network, adversary can adopt different attack strategies. However, not all attack strategies are applicable in all types of wireless sensor networks. For example, routing attacks are not applicable in network scenarios, where each sensor node communicates with the central server directly.

Key management is the most important part of WSN security. Apart from maintaining confidentiality, it also assists other modules such as authentication, privacy and sometimes integrity. Therefore it is important to have key management strategy, which provides security as per the requirements of target WSN application and also incurs less overhead on sensor nodes. Considering the diversity in WSN applications and network topologies in WSN, it is highly unlikely that one scheme outperforms all other schemes in all the scenarios. Therefore, we feel that it is necessary to survey possible applications of WSN, their effects on the underlying WSN and efficacy of existing key management solutions in each scenario. There are two main contributions of this paper: Firstly, we have classified wireless sensor network into different scenarios according to its possible applications. Secondly, we have identified the most appropriate key management scheme for each scenario of wireless sensor network.

Rest of the paper is organized as follows: In section 2, we will discuss various applications of wireless sensor networks and effects of their characteristics and requirements on the underlying sensor network. In section 3, we will discuss all possible threat possibilities in WSN and threat possibilities in each network scenario described in section 2. In section 4, we will discuss key management schemes of WSN and their effectiveness in each scenario of wireless sensor network. Before conclusion, we will provide quantitative comparison of key management schemes in each scenario of wireless sensor network in section 5. In the end, section 6 will conclude the paper.

## 2. APPLICATION DEPENDENT NETWORK CHARACTERISTICS AND TOPOLOGIES

There are a lot of applications, for which sensor networks are employed. These applications range from military surveillance, in which a large number of sensor nodes, possibly densely deployed, are used, to health care applications, in which a very limited number of sensor nodes can be used. Naturally, these applications have an impact on the specifications of the employed sensor nodes and characteristics and topologies of the underlying sensor networks.

### 2.1 Sensor Network Application Scenarios

In this subsection, we will list all possible applications, in which sensor networks can be employed. Also, we will discuss specifications of the employed sensor nodes and characteristics and topologies of the sensor networks employed in these application scenarios. In this respect, some researchers have tried to identify possible application scenarios of wireless sensor networks [Xu 2002; Cantoni et al. 2007; Ruair et al. 2008]. We have tried to extend their list of possible application scenarios by carrying out extensive literature review. We have listed significant publications from the reviewed literature under the heading of each category of possible application scenarios.

2.1.1 *Habitat and environment monitoring*. Habitat and environment monitoring are the most important applications of wireless sensor networks. In fact, these are the applications, for which wireless sensor networks were designed primarily. Numerous researches have identified these application areas for wireless sensor networks [Mainwaring et al. 2002; Holman et al. 2003; Martinez et al. 2004], challenging issues in them and their solutions [Estrin et al. 1999; Braginsky and Estrin 2002; Akyildiz et al. 2005].

In such applications of wireless sensor networks, the number of nodes depends upon the physical dimensions of the area, on which a wireless sensor network is employed. For example, if an application needs to monitor soil moisture at different places in a field of crops, it will need a large number of nodes. However, normally a large number of nodes are used in such applications in order to increase robustness and reliability. In fact, this is the reason why the cost of a sensor node is kept low. Reducing the cost of a single sensor node ensures that a large number of nodes can be used.

Node density in habitat and environment monitoring varies from application to application. In applications, in which it is possible to retrieve sensor nodes and change their batteries, user might choose to use a small number of nodes, with reasonable communication capabilities and place them at strategically important positions. Node density might be even less if the terrain is not very hostile because extra nodes are not required in many terrains. On the other hand, there are many applications, in which it is not possible to retrieve sensor nodes. For example, if sensor nodes are deployed in some volcanic area, it is not possible to retrieve them and replenish their batteries. Also, there are chances of loosing nodes during operation. In such terrains, node density is kept high.

In habitat and environment monitoring applications, nodes in wireless sensor networks are normally static. However, there are many applications, in which the nodes are mobile and the network topology does not remain the same all the time. For example, in an ocean monitoring application, sensor nodes can be moved from one place to another. It is important to develop protocols for such scenarios as well.

2.1.2 *Surveillance*. Apart from monitoring environments and habitats, wireless sensor networks have been used for military and non-military surveillance. Surveillance applications are not exactly the same as monitoring applications. In monitoring applications, data is transferred to the base station at regular intervals. However, it may not be like this in surveillance applications. In surveillance applications, communication is mostly event-driven rather than being regular. Many researchers have identified research challenges in surveillance applications of wireless sensor networks [Gui and Mohapatra 2004; He et al. 2004] and proposed their solutions [Yan et al. 2003; Chakrabarty et al. 2002; He et al. 2006].

Number of nodes in surveillance applications is usually large because it is not feasible to use a small number of nodes to track an object or an event. For example, if a wireless sensor network is used to track panda, tiger or other animals in a forest, a large number of nodes should be deployed strategically at various positions. It is important to do it in such a way so that an animal can be monitored effectively.

For all surveillance applications, a large number of nodes is required. However, all surveillance applications of wireless sensor networks need not have similar node density. In military applications, node density is always high because of hard terrain and high possibility of attacks on the employed sensor network. In other surveillance applications, node density can be low. For instance, if a wireless sensor network application tracks a particular animal of an endangered species in a particular patch of forest, node density can be less if nodes are carefully placed at strategically important positions. There is a high possibility that an illegal hunter tries to hunt an animal from endangered species. In order to avoid recording of an evidence, the illegal hunter tries to track down the sensor node and destroy or disable it. It is important to have extra sensor nodes to improve reliability in such networks. This can be achieved by effectively hiding redundant nodes in the environment or by deploying such a large number of nodes that it becomes practically impossible for the adversary to stop the information from flowing to the base station.

Although sensor nodes can be mobile in non-military surveillance application of wireless sensor networks, normally the network dynamics do not change. However, network topologies can change dynamically in military applications. Hidden sensor nodes can be forced to change positions following an explosion or some other unforeseen event. Also, if sensor nodes are implanted on bees they are deemed to have dynamic network topology.

2.1.3 *Smart homes and offices*. Apart from the use of wireless sensor networks in possibly hard terrains for monitoring and surveillance, they can be used indoors to assist human beings, provide them with a better lifestyle [Ward et al. 1997; Noury et al. 2000; Intille 2002; Cook et al. 2003] and help them in their problems. For example, sensor networks can be used for monitoring activities of elderly and ill people within their homes [Barger et al. 2005]. Although we consider wearable sensor nodes as part of body area sensor networks (refer to section 2.1.5), they can assist in making office and homes smart [Clarkson et al. 2000].

It may seem as if only a small number of sensor nodes are required for indoor applications as compared to the outdoor applications. However, this is totally application dependent. For example, application involving smart kitchen appliances will have a higher number of nodes as compared to the applications that only monitor the activities of a person living inside a house or working in an office. Similarly, node density also depends upon the application.

In most cases of indoor applications, sensor networks are static. However, there may be cases when some sensor nodes does not remain at one place. For example, if a person is wearing a sensor node, it will be mobile and sensor network protocols must take care of the mobility of such sensor nodes.

An important difference between the outdoor sensor networks and the indoor sensor networks is that the batteries of all indoor sensor nodes can be replenished. In addition to that, some static sensor nodes may not even require batteries to operate. For example, a sensor that is permanently fitted on walls for tracking a person, can use power directly from the electric supply.

2.1.4 *Industrial process control*. Industrial process control is another class of indoor applications of wireless sensor networks [Estrin et al. 1999; Nilsson et al. 2008]. In fact, these class of applications can be classified as indoor as well as outdoor because of the size of industrial plants. Sensor nodes can be deployed in those areas of an industrial plant, which cannot be accessed easily and frequently.

The number of sensor nodes employed in industrial process control systems vary according to the size of industrial plant. A small plant can be controlled with fewer nodes without even deploying redundant nodes for resilience. However, if we employ a sensor network for plants that span large areas, we might need a network with a large number of nodes, possibly with a higher node density.

Node mobility is not a big issue in applications involving industrial process control. Mostly, sensor nodes are fixed at their positions. There may be some mobile nodes in these scenarios. For example, entry of a node in a certain area may trigger some actions. However, this mobility does not have an effect on the dynamics of the network. For instance, sensor network protocols do not have to cater for scenarios, in which unknown nodes try to establish connections very frequently.

Sensor nodes used in industrial process control applications might have power options available for them. For example, some nodes might be able to get power from electric supply directly. Also, it may not be possible to replenish batteries of all sensor nodes. For example, some nodes may be deployed in such areas, which are not very frequently accessible. Sensor network protocols need to cater for such scenarios.

2.1.5 *Body area sensor networks*. This is a very special scenario of wireless sensor networks. Although it is also an indoor application of wireless sensor networks, it has some unique characteristics, due to which it should be treated separately. All sensor nodes, in a body area sensor network, are placed on a body, which is a human body in most cases [Jovanov et al. 2005]. Sensor nodes are very close to each other.

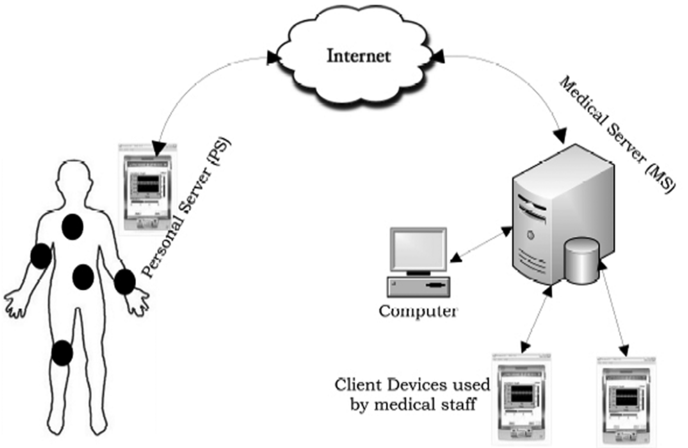


Figure 2. Application Environment for Wireless Body Area Sensor Networks. Black circles on the body depict sensor devices used for monitoring biometrics. Sensor devices forward their readings to a PS through wireless links. PS uses wired or wireless internet connection to communicate patient's information to an MS located in a clinic or a hospital. Finally, authorized medical staff can use wired or wireless connection to access patients' real-time information on the MS.

Different sensor nodes have been designed for such sensor networks [Gyselinckx et al. 2005; Klemm and Troester 2006] and separate protocols have been defined [Otto 2006]. Also, researchers have been studying the effect of the presence of human body on such sensor networks [Zasowski et al. 2003; Timmons and Scanlon 2004]. Apart from these differences, there is difference in application characteristics, which helps in the key management for such networks [Raazi et al. 2009].

Scale of body area sensor networks is very small because of their usability. A patient, in health care environment, or an elderly person, in life care environment, might refuse to wear a large number of devices on their bodies. Node density cannot be large with a few sensor nodes and network topology cannot be changed in these circumstances. Although the nodes can't be charged from electric power directly, all the nodes are accessible to human beings and their batteries can replaced at any time. Personal applications, running on mobile devices, can also use biometrics information [Augusto Celentano and Pittarello 2009]. Figure 2 visions an environment, in which wireless body area sensor networks are used. Also, different data mining strategies are employed on medical server to make use of data from health care applications [Yoo and Song 2008].

### 2.2 Network Classification

In this subsection, we will classify sensor networks based upon their characteristics. Our classification will depend upon the discussion of the previous subsection 2.1. In the previous subsection, we may not have listed all application scenarios of wireless sensor networks but we think that most application scenarios would fall under one of the categories that we have listed. Instead of just listing the possible application scenarios, our purpose is to extract the characteristics of the underlying network in each scenario and then classify wireless sensor networks according to the network characteristics. After the discussion in the previous subsection, we classify wireless sensor networks as follows:

2.2.1 *High density, static sensor networks (HDSSN).* After the discussion in the previous subsection, we find that the most common class of sensor networks has a large number of low cost nodes scattered around the target area with a high node density per unit area. In this class, sensor nodes are not mobile and the network topology remains stable. In this case, sensor nodes do not get power from an electric source directly. We do not classify this type of sensor network any further on the basis of whether the energy sources of the sensor nodes can or cannot be replenished. Reason is that in both cases the protocols, designed for such sensor networks, must be energy efficient. We use abbreviation HDSSN for this class of sensor networks.

2.2.2 *High density, dynamic sensor networks (HDDSN).* In a typical high density sensor network, it is quite possible that the network topology does not remain stable as discussed earlier subsections 2.1.1 and 2.1.2. As these are high density networks, the number of nodes is always high in this type of wireless sensor network. In this case also, sensor nodes do not get power from an electric source directly and the protocols designed for such sensor network should be energy efficient irrespective of whether energy sources of the sensor nodes can be replenished or not. We use abbreviation HDDSN for this class of sensor networks.

2.2.3 *Energy constrained, low density, static sensor networks (ECLDSSN).* This is another type of sensor networks that can be classified separately. In this case, sensor nodes are not very close to each other but they are fixed at their positions. This type of sensor network may not have many redundant sensor nodes. It may or may not be possible to replenish the energy supplies for the sensor nodes in these networks. However, energy supply is not available from an electric source directly. This class of sensor networks could have been classified further on the basis of the number of nodes in a network. However, this classification would not be fruitful because this would not have an effect on the working of sensor network protocols. In the remaining text, abbreviation used for this class of sensor networks will be ECLDSSN.

2.2.4 *Unlimited energy, static sensor networks (UESSN).* There are cases, in which sensor nodes can be fixed at their locations in a home, processing plant or an office. It is possible to supply direct electric power to these static nodes. This has a direct effect on the protocols designed for such sensor networks. However, unlimited energy does not have an effect on other constraints such as computation power, communication power and memory. The number of nodes in such networks varies according to the application. It may be small in case of smart home or office but it may be high if used in a large industrial processing plant. However, node density of this type of sensor network is always low. In the remaining text, abbreviation used for this class of sensor networks will be UESSN.

2.2.5 *Low density, dynamic sensor networks (LDDSN).* This is not a very common scenario in wireless sensor networks. However, it is a valid scenario and future applications might use such type of networks. In this case, sensor nodes are mobile and the network topology is dynamic. Such networks can be formed in large offices, with a wearable sensor on every person. It is important not to confuse this class of sensor network with the scenario, in which mobile sensor nodes move in and out of the communication range of each other but rarely come across stranger nodes. We classify such scenario under ECLDSSN because communication paths are fixed and are activated when sensor nodes come in communication range of each other. We abbreviate the low density, dynamic sensor networks with LDDSN.

2.2.6 *Wireless body area networks (WBAN).* This is the most unusual class of wireless sensor networks. In this case, a small number of sensor nodes are placed in close vicinity of each other. All nodes always remain in the communication range of each other. The number of nodes cannot be large because of the usability issue. Perhaps, the number of nodes used in a WBAN may increase in future, when scientists discover ways to implant large number of microsensors inside or around human body. We do not classify these sensor networks under ECLDSSN because different protocols are designed for such networks due to their distinct characteristics as discussed in previous subsection.

## 3. THREAT POSSIBILITIES IN DIFFERENT WIRELESS SENSOR NETWORK TOPOLOGIES

In the previous section we have been able to classify wireless sensor networks under six classes according to the applications of wireless sensor networks. In this section, we will identify the threat possibilities and their applicability in each class of sensor networks. This will help us in understanding how the requirements for key management change in different scenarios.

Main goal of key management is to maintain confidentiality of information. Keys can also assist in authenticating legitimate nodes and checking the integrity of the transferred messages. Adversaries try to guess secret keys and get access to the confidential information. In order to avoid adversaries from getting access to secret information, it is important to refresh the secret keys at regular intervals, which depend upon the frequency of communication and frequency of key usage.

Guessing the key is not the only way, in which an adversary tries to affect a sensor network. It can launch Denial-of-service attacks on the network. It can disrupt communication or try to drain energy of sensor nodes by sending bogus messages or by replaying old messages. Likewise, many attacks are possible on sensors [Zia and Zomaya 2006]: -

### 3.1 DoS (Denial of Service) Attacks

Denial of service attacks are carried out with the help of an outsider node, which disrupts the communication channel between the communicating sensor nodes. Jamming attack is a type of DoS attack. Jamming is an attack on the physical layer and can be launched on any type of sensor network. Key management schemes can't take care of jamming attacks as they occur on the physical layer. There are other methods to take care of such attacks. Such methods are out of the scope of this paper. These attack does not remain significant in those sensor networks, in which timely human intervention is possible. For example, if an attacker node is detected in a smart home or office environment, it can be physically removed by human beings. Human intervention is mostly possible in sensor networks, which belong to the WBAN class. However, it cannot be guaranteed.

### 3.2 Passive Information Gathering and Message Corruption

In these attacks, adversary listens to the information passively. It can also try to corrupt the messages being exchanged between different nodes. These attacks are applicable on all the six classes, which we have defined, of wireless sensor networks. Effective key management mechanisms can take care of such attacks on sensor networks.

### 3.3 Node Compromise

An adversary can exploit a hole in the system software of a sensor node to gain control of the node. After gaining control of the sensor node, the adversary can access all the data and information stored on the sensor node. Cryptographic keying material are also lost. Compromised node can listen to the communication between other nodes, interrupt communications, intercept messages, modify and fabricate messages.

This attack can take place in all classes of sensor networks. It has less effect on those networks, in which human intervention is possible. In such networks, compromised nodes can be physically removed or turned off. However, it is important to include a strategy for node eviction in every key management schemes as human intervention is not always possible.

### 3.4 Node Tampering

In this case, an adversary gets hold of a sensor node physically and gains access to all data, information and important cryptographic material. When a node is tampered, it is compromised physically and it can be used to listen to communications, interrupt them, intercept, modify and fabricate messages. This attack can also happen in all classes of sensor networks. This attack cannot happen in physical presence of human being. However, physical presence of human being cannot always be guaranteed. Therefore, key management scheme should have mechanisms to cater for such attacks.

### 3.5 False Node

In this case, an illegitimate node is introduced in a sensor network. It tries to act as a legitimate node, tries to inject false data in the network or tries to attract data towards itself. For example, it can inject false routing information in the network, so that all nodes route their packets through the illegitimate nodes. Although HDSSN, HDDSN and LDDSN are most likely targets of this attack, this attack can take place in all classes of sensor networks.

### 3.6 Node Outage

In node outage attack, adversary removes the node from the network or drains all its energy. It can happen in all classes of sensor networks. Human presence hampers the adversary from carrying out such an attack. Key management schemes cannot take care of node outage attacks. Therefore, it is out of the scope of this paper.

### 3.7 Traffic Analysis

Adversary can passively analyze the traffic patterns in a sensor network. This can lead to a calculated attack on a sensor network. For example, if all the traffic is routed through a single node, adversary can attack that node and bring down the network. Although traffic analysis attack has higher repercussions on HDSSN, HDDSN and LDDSN, it is applicable to ECLDSSN, UESSN and WBAN as well.

### 3.8 Acknowledgement Spoofing

An attacker node can spoof the acknowledgement of a data packet, which has not been transferred to the receiver successfully. This hampers the information from getting to the sink node. Either the receiver node is dead or it is barred from receiving the data packet in some other way. It is equally applicable to all classes of sensor networks except WBAN. This is because in WBAN, sink node is inside the communication range of all the nodes and data packets are not routed through other nodes. Sink node is not energy constrained as other nodes.

### 3.9 Spoofed, Altered or Replayed Routing Information

A compromised node is used to play with the routing information and disseminate false routing information through a sensor network. This attack is more likely to occur in HDSSN, HDDSN and LDDSN but cannot be ruled out from ECLDSSN and UESSN. These attacks are not applicable to WBAN because packets are not routed through other nodes in WBAN.

### 3.10 Selective Forwarding

A false or compromised node is used to create a black hole in the target sensor network. False or compromised node deliberately drops data packets to disrupt network operation. This kind of attack is more likely to occur in HDSSN, HDDSN and LDDSN but cannot be ruled out from ECLDSSN and UESSN. It is not applicable to WBAN because it involves routing.

### 3.11 Sinkhole Attacks

This is similar to selective forwarding except that it is not a passive attack. In this case, traffic is attracted towards the compromised or false node. Applicability of sinkhole attack is the same as that of selective forwarding.

### 3.12 Sybil Attacks

In sybil attacks, malicious node presents multiple identities to the sensor network either by creating them or by stealing the identities of other nodes. It is equally applicable to all classes of sensor network. In WBAN, it can use false identities to send false information to the base station. In other classes of sensor networks, it can cause a routing algorithm to calculate two disjoint paths.

### 3.13 Wormhole Attacks

Two distant malicious nodes are used to create a wormhole in the target sensor network. Both malicious nodes have an out of band communication channel. One node is placed near the sensor nodes. It advertises shortest path to the sink node through the other one, which is placed near the sink node. This creates sinkholes and routing confusions in the target sensor network. Applicability of wormhole attacks is the same as that of selective forwarding and sinkhole attack.

### 3.14 Hello Flood Attacks

In hello flood attack, a malicious node plays or replays a hello packet with a high signal strength in the target sensor network. High signal strength makes all other nodes think that the malicious node is their neighbour. It then creates a wormhole. Also, other sensor nodes loose their energy in replying to the hello packet. Although creation of wormhole does not affect the WBAN, it does cause sensor nodes to reply to the hello packet in WBAN. Therefore, it is applicable to all classes of sensor networks.

## 4. KEY MANAGEMENT SCHEMES AND THEIR EFFICACY IN DIFFERENT APPLICATION ENVIRONMENTS

Before this section, we classified wireless sensor networks in different categories. Then we discussed different types of attacks that can take place in wireless sensor networks and their applicability in different categories. We learned that all types of attacks are applicable to all the classes of sensor networks except WBAN. This is due to the network characteristics of WBAN. Later, we will see that separate key management schemes are designed for WBAN due to the differences in application and network characteristics of WBAN from all other classes of sensor networks.

In this section, we will discuss various key management schemes provided in the literature so far. In this regard, work of [Xiao et al. 2007] is of great importance. While discussing the key management scheme, we will also discuss their effectiveness in each class of sensor networks.

### 4.1 Single Network-wide Key

This is the simplest scheme that can be devised for any class of wireless sensor network. In this case, a single key is stored on every node and all nodes use that key to secure communications. Communication overhead is minimal if we use one group key for the whole network. Also, there is very little computation and storage overhead involved. Drawback of this scheme is that if a single node is compromised, the secret key is revealed and the whole network is compromised. Also, it is very weak against cryptanalytic attacks.

This key management scheme is equally applicable to all classes of wireless sensor networks. It is not advisable to use this key management scheme in any class of sensor networks because of its vulnerability. However, this key management scheme can be the best option for some applications of HDDSN and LDDSN, in which node mobility is very high. To reduce vulnerability, a variant of this scheme can be used for HDDSN and LDDSN. Variation is that we use more than one network-wide keys so that if one key is compromised, nodes can continue to communicate using other keys. Yet another variation can be that different keys are used in different physical areas of HDDSN or LDDSN and mobile nodes posses keys for all those areas, in which they can move.

### 4.2 Pair-wise Key Establishment

In this scheme every node shares different secret key with all other nodes in the network. For example, if there are $n$ nodes in a network, every node stores $n$–1 keys in its memory. It might not impose large communication and computation overheads on the sensor nodes but it does impose a large storage overhead. This scheme is highly secure but not scalable at all.

This is also a very simple solution for any class of wireless sensor networks. However, it establishes communication paths between all the nodes, even the ones, which do not need to communicate. Most certainly, this scheme is not meant for large sensor networks like HDSSN and HDDSN. Although it is not efficient for WBAN but this scheme is usable in WBAN as WBAN has a very small number of nodes. It is a viable solution in ECLDSSN, UESSN and LDDSN, too if the number of nodes remains under a certain limit. If LDDSN has a small number of nodes, this solution might be the most viable one if sensor nodes can bear its storage overhead.

### 4.3 Random Pair-wise Key Establishment

Following the shortcomings of pair-wise key establishment scheme, random pair-wise key establishment scheme was proposed [Chan et al. 2003]. It was based on the fact that all pairs of sensor nodes in a wireless sensor network do not need a communication path between themselves. In this scheme, any pair of sensor nodes share a common key with some probability *p*, which must be chosen carefully in order to keep network connectivity up to a desired level. In this work, it is proposed that the base station is not required to evict a compromised node. If there is a consensus among its neighbouring nodes that a certain node is compromised, all nodes stop their communication with that node and treat it as an outsider. Compromised nodes cannot listen to the communication between other nodes as different key is used between every pair of nodes.

This scheme is more efficient than the simple pair-wise key establishment scheme. However, still it is not scalable and not advisable for networks with large number of nodes like HDSSN and HDDSN. Also, it is not suitable for UESSN and ECLDSSN because it can happen that two nodes, who share a common key, are located at two extreme ends of the sensor network. In this case, such keys would needlessly occupy space in sensor nodes' memory. In WBAN, all nodes communicate with the base station directly and communication with other nodes is not important. So, this scheme is usable but not efficient for WBAN scenario. Although this key management scheme seems to be a better solution than simple pair-wise key establishment scheme for LDDSN, it requires a variation. Neighbours are not fixed in LDDSN, so the news of compromised node detection should be broadcasted to the whole network rather than only a few neighbouring nodes.

### 4.4 Trusted Key Distribution Center (KDC)

Pair-wise key management schemes based on trusted key distribution center introduce mechanisms for node authentication. In pair-wise key establishment schemes, pair-wise keys are preloaded on sensor nodes and the neighbouring sensor nodes start communication with each other directly. In this scheme, all pair-wise keys are stored on a trusted server. This server can be the base station or a sensor node. Every pair of nodes contact the trusted node to obtain a pair-wise key for every session. This scheme is resilient against node capture and node replication. However, there are many drawbacks of this scheme. This scheme imposes high communication overhead, high storage overhead on the trusted node and can cause congestion on the links around the trusted node. In addition to that, it requires the trusted node to have more capabilities than other sensor nodes and it causes the trusted node to become a single point of failure for the network.

This scheme is certainly not suitable for sensor networks having large number of nodes like HDSSN and HDDSN as it is not scalable. It is not possible to store such a large number of keys of a sensor node, and it will cause a lot of communication overhead. It can be useful in UESSN and ECLDSSN only with a small number of nodes. This scheme does not suit WBAN because in WBAN, all nodes need to communicate with the base station most of the time. Communication between other nodes is not very common. With a small number of nodes and small physical area of operation, this scheme can prove to be useful for LDDSN.

### 4.5 Random Key Pre-distribution Scheme

We have already discussed that in a wireless sensor network, it does not matter if all pairs of sensor nodes do not have a communication path between each other. However, it is important that every sensor node has ample communication paths leading to the base station. In random key pre-distribution scheme [Eschenauer and Gligor 2002], a key-chain is stored in every sensor node. All keys are group keys, which the base station shares with a group of sensor nodes. Upon deployment, every sensor node can only communicate with those sensor nodes, with which it shares a secret key. Also, if a node has a redundant key after network initialization, it can use that key to establish communication path between two other nodes, which do not share a common key. If a node is compromised, the base station broadcasts the list of keys that it possesses. All other nodes delete these keys from their memories. A drawback is that communication links, not directly related to the compromised nodes, are also affected.

Although efficiency of random key pre-distribution scheme can be argued, it is equally applicable to all static sensor networks like HDSSN, UESSN and ECLDSSN except WBAN because WBAN does not need to establish multiple communication paths with the base station. For HDDSN and LDDSN, this is a very efficient and suitable key management solution because any pair of nodes can establish a communication path between themselves without the overhead of having pair-wise keys as well as the vulnerability of having a single group key.

### 4.6 Q-Composite Random Key Pre-distribution Scheme

In order to cater for the drawback of random key pre-distribution scheme, Q-composite random key pre-distribution scheme was proposed [Chan et al. 2003]. In this case, if two nodes need to communicate with each other, they must share at least $q$ number of keys. When a compromised node is evicted and its keys are revoked, other links remain unaffected. However, the key pool is reduced to maintain the probability that two nodes share $q$ common keys. So, the adversary would need to compromise a few nodes to compromise the whole network.

Applicability of this scheme on HDSSN, UESSN, ECLDSSN and WBAN is the same as the random key pre-distribution scheme. For LDDSN and HDDSN, random key pre-distribution scheme is more usable than Q-composite random key pre-distribution scheme. This is because of the fact that nodes in dynamic sensor networks do not need to establish permanent communication links. Therefore, it is better to have a scheme that has a larger key pool rather than the one, which focuses on establishing permanent communication links between the sensor nodes.

### 4.7 Multi-path Key Reinforcement Scheme

In multi-path key reinforcement scheme, multiple paths are established between two communicating nodes [Chan et al. 2003]. As an example, consider that two nodes $A$ and $B$ have $h$ disjointed paths between them and they use key $k$ for communication. One node sends $h$ different random values to the other node through separate paths. Then they both compute a key $k'$ using key $k$ and $h$ random values. If key $k$ is compromised, they refresh it using $k'$.

This scheme increases the computation overhead of sensor nodes, which drains precious energy. For UESSN, this scheme is better than random key pre-distribution and Q-composite random key pre-distribution schemes because of increased security. For HDSSN and ECLDSSN, this security comes at an additional cost. This key management scheme is not applicable for WBAN, LDDSN and HDDSN because there are direct communication links with the base station in WBAN and dynamic sensor networks do not have permanent communication paths between sensor nodes.

### 4.8 Polynomial Pool-based Key Pre-distribution

In this case, one polynomial of degree $t$ is assigned to each sensor node [Liu and Ning 2003]. The polynomial has a property that $f(x, y) = f(y, x)$. If nodes $i$ and $j$ receive polynomials $f(i, y)$ and $f(j, y)$, respectively, they can compute a common key using identity of the other node. This is a scalable scheme but whole network is compromised if $t$ nodes are compromised.

This scheme suits large-scale sensor networks because of its scalability and dynamic sensor networks because of its ability to establish connection with unknown sensor nodes. Therefore, it is suitable for HDSSN, HDDSN and LDDSN. It is suitable for UESSN and ECLDSSN if the number of nodes is high. For other networks, especially WBAN, this scheme is not suitable.

### 4.9 Public Key Cryptography in Wireless Sensor Networks

Public Key Cryptography schemes require highly sophisticated computation, which consumes precious energy from sensor nodes. Most researchers argue that public key cryptography should not be used in wireless sensor networks because of excessive computation costs. However, some researchers argue that public key cryptography especially elliptic curve cryptography (ECC) cannot be ruled out of wireless sensor networks [Gura et al. 2004; Malan et al. 2004; Wandar et al. 2005]. According to [Gura et al. 2004], 160-bit ECC provides the same level of security as 1024-bit RSA [Rivest et al. 1978] and the difference in the number of bits is exponential because 224-bit ECC provides the same level of security as 2048-bit RSA.

Hybrid approaches have also been proposed for wireless sensor networks. In hybrid approaches, both symmetric and asymmetric keys are used [Huang et al. 2003]. Public key cryptography is not viable to use in those sensor networks, which have large number of nodes. It is viable for sensor networks, having small number of nodes especially if they fall under the category of UESSN. It is viable to use public key cryptography in HDDSN and LDDSN but not in WBAN.

### 4.10 SHELL

SHELL scheme is designed for large scale clustered sensor networks [Ghumman 2006]. SHELL makes use of EBS matrix [Eltoweissy 2004] to manage a large number of nodes using a small number of keys. SHELL supports in-network-processing [Karlof et al. 2003; Madden et al. 2002] and avoids single point-of-failure in a network by involving cluster heads nodes of neighbouring clusters for key management.

An EBS system of matrices stores information about keys stored on every node. There are a total of $k+m$ keys, out of which every node knows a distinct set of $k$ keys. If a node is compromised, $m$ keys, which are not known to the compromised node, are used to refresh the $k$ compromised keys to evict the compromised node. Total number distinct sets of $k$ keys can be depicted by this formula: -

$$n = \frac{(k+m)!}{k!m!} \tag{1}$$

In SHELL, cluster head node of a cluster generates the EBS matrix, breaks it up into different parts and sends those parts to its neighbouring cluster head nodes. Neighbouring cluster head nodes manage keys for the cluster. The EBS matrix is divided in such a way that the compromise of a neighbouring cluster head node does not compromise too many keys. On a cluster head's request, neighbouring cluster heads generate keys and refresh them. However, the cluster head node does not get to know the actual key values.

SHELL is an ideal key management scheme for HDSSN. Also, it is a very viable solution for those HDDSN, in which node mobility is low i.e. within the area of a defined cluster. This is a workable but not efficient solution for other classes of sensor networks like ECLDSSN, UESSN and LDDSN. For WBAN, this solution is not always usable because WBAN does not necessarily have neighbouring clusters. Also, the number of nodes is very small in WBAN.

### 4.11 MUQAMI+

MUQAMI+ is also an EBS based key management scheme for large scale clustered sensor networks [Raazi et al. 2009]. In this scheme, responsibility of key management is distributed within the same cluster and inter-cluster communication is avoided. Also, computation and storage overhead is reduced. Single point of failure is avoided by distributing the responsibility of key management among a small fraction of nodes within the cluster. This is done with the help of one-way hashing [Lamport 1981] functions and key-chains [Dini and Savino 2006].

Although the CH node stores the EBS matrix, it does not get to know the actual key values. Even in the case of node compromise, messages are sent through the CH node but the key values are not revealed to it in order to maintain the property of not having a single point of failure in a cluster. Also, responsibility of being cluster head node or generating keys can be shifted from one node to another with minimal overhead.

Applicability of MUQAMI+ to HDSSN and HDDSN is the same as that of SHELL. This scheme is ideal for use in HDSSN and HDDSN, with limited mobility. For all other classes of sensor networks including WBAN, MUQAMI+ is a workable but inefficient key management solution.

### 4.12 LEAP+

LEAP+ [Zhu et al. 2006] is a key management solution that is not targeted towards some specific class of sensor networks. In LEAP+, each node's cluster consists of all its neighbours. In this scheme, every node stores 4 types of keys. One key is shared with the base station. After deployment, every node establishes keys with all its neighbours. After that, it shares another key with all neighbours for broadcast purposes. Finally, there is a single network-wide key used for broadcast purposes in the whole network. If a node is compromised, its neighbouring nodes delete pair-wise keys shared with it, then refresh their group keys, which they use for broadcast purposes. In the end, network-wide key is refreshed.

LEAP+ is a key management solution, that is equally applicable to almost all classes of static sensor networks. It is ideal for use in ECLDSSN and UESSN. Also, it is a very scalable key management scheme and is useful for HDSSN. However, it is not suitable for WBAN and not applicable in dynamic sensor networks. It is not suitable for WBAN because all nodes do not need to establish communication paths with all its neighbours while in LEAP+, every node established communication links with all its neighbours. In dynamic sensor networks like HDDSN and LDDSN, nodes are mobile and neighbourhood changes dynamically. If LEAP+ is used when neighbourhood is not static, nodes will consume a lot of energy in establishing communication links with other nodes. Therefore, it is not feasible to use LEAP+ in dynamic sensor networks.

### 4.13 Plug'n Play Key Management for WBAN

In the discussion up till now, we have seen that the applicability of any key management scheme in WBAN is different from its applicability in other classes of sensor networks. This is mainly because of the topology and scale of WBAN. From topology and scale, WBAN resembles WPAN. However, WBAN is used to measure biometrics from human body, which has an effect on communication between sensor nodes planted on human body [Zasowski et al. 2003; Timmons and Scanlon 2004]. Also, biometrics from human body exhibit certain randomness properties, which help in key management [Poon et al. 2006; Cherukuri et al. 2003].

[Falck et al. 2007] proposed a solution for key management in WBAN based on the above mentioned research and studies. They proposed that the communicating sensor nodes do not even need to exchange keys in order to establish a communication link. In this scheme, two sensor nodes sense the same biometric at a particular time instant and then use error correcting codes to compute final key values. Error correcting codes remove the possible differences that may arise in the readings of the two nodes.

This key management scheme is specifically designed for WBAN and is not applicable to other classes of wireless sensor networks. Although it is designed for specifically for WBAN, it is a primitive scheme and has many shortcomings.

### 4.14 BARI

BARI [Raazi et al. 2009a] covers the shortcomings of the existing key management solutions for WBAN. Apart from time synchronization and other issues in error correcting codes, two sensor nodes are supposed to sense a single biometric in [Falck et al. 2007]. This is not always possible because any other human being might refuse to wear more than a certain number of devices. Also, one device is used to measure one biometric most of the time. Devices, measuring multiple biometrics might have financial implications.

In BARI, it is assumed that a small number of nodes are placed on human body and each node senses its own biometric. The base station, also called the personal server, issues a key refreshment schedule. Every node refreshes the key on its turn. When all nodes have taken their turn, new refreshment schedule is issued by the base station. Even though node compromise is not very common in such indoor human attended environments, BARI has a provision for evicting compromised nodes.

BARI is designed specifically for WBAN environments. However, its variant can be used in UESSN. In UESSN, a few communicating nodes near to each other can take turns to refresh keys. BARI is not a viable key management scheme for all other classes of sensor networks except LDDSN. Even in LDDSN, it is a viable solution if node mobility is low.

Table I. Applicability of Every Key Management Scheme in Each Scenario of Wireless Sensor Networks.

| Scheme | HDSSN | HDDSN | ECLDSSN | UESSN | LDDSN | WBAN |
|---|---|---|---|---|---|---|
| Single Network-wide Key | Yes | Yes | Yes | Yes | Yes | Yes |
| Pair-wise Key Establishment | No | No | Yes | Yes | Yes | Yes |
| Random Pair-wise Key Establishment | No | No | Yes | Yes | Yes | Yes |
| Trusted Key Distribution Center (KDC) | No | No | Yes | Yes | Yes | No |
| Random Key Pre-distribution | Yes | Yes | Yes | Yes | Yes | No |
| Q-Composite Random Key Pre-distribution | Yes | Yes | Yes | Yes | Yes | No |
| Multi-path Key Reinforcement | Yes | No | Yes | Yes | No | No |
| Polynomial Pool-based Key Pre-distribution | Yes | Yes | Yes | Yes | Yes | No |
| Public Key Cryptography | No | Yes | Yes | Yes | Yes | No |
| SHELL | Yes | No | Yes | Yes | No | No |
| MUQAMI+ | Yes | No | Yes | Yes | No | Yes |
| LEAP+ | Yes | No | Yes | Yes | No | Yes |
| Plug'n Play Key Management for WBAN | No | No | No | No | No | Yes |
| BARI | No | No | No | Yes | No | Yes |

In Table I, we summarize the applicability of each every management scheme in each scenario of wireless sensor network. We assume that for a scheme to be applicable in dynamic wireless sensor networks, it should be able to accommodate high node mobility. Apart from only being able to provide basic protection i.e. help in maintaining confidentiality and integrity of information and authenticating the users through secret keys, a key management scheme should be able to refresh keys in a secure way and evict malicious nodes from the network whenever necessary. A key management scheme may be more energy efficient as compared to other schemes but provide less security services as compared to other schemes. Therefore, it is important to compare the security services provided by each key management scheme. In Table II, we compare the services provided by each key management schemes discussed in this paper.

Table II. Comparison of Services Provided by Each Key Management Scheme.

| Scheme | Basic Protection | Key Refreshment | Node Eviction |
|---|---|---|---|
| Single Network-wide Key | Yes | No | No |
| Pair-wise Key Establishment | Yes | No | No |
| Random Pair-wise Key Establishment | Yes | No | No |
| Trusted Key Distribution Center (KDC) | Yes | Yes | Yes |
| Random Key Pre-distribution | Yes | No | No |
| Q-Composite Random Key Pre-distribution | Yes | No | No |
| Multi-path Key Reinforcement | Yes | Yes | No |
| Polynomial Pool-based Key Pre-distribution | Yes | No | Yes |
| Public Key Cryptography | Yes | Yes | No |
| SHELL | Yes | Yes | Yes |
| MUQAMI+ | Yes | Yes | Yes |
| LEAP+ | Yes | Yes | Yes |
| Plug'n Play Key Management for WBAN | Yes | Yes | No |
| BARI | Yes | Yes | Yes |

When deciding an appropriate key management scheme for any scenario of wireless sensor network, it is important to choose a scheme that provides maximum security services. After that, we should focus on efficiency. For HDSSN and ECLDSSN, many schemes are applicable but only few provide all security features. For HDSSN, MUQAMI+ may be the most appropriate scheme if the network is collusion resistant. If the network is not collusion resistant, LEAP+ may be the most appropriate scheme because SHELL and MUQAMI+ are not collusion resistant schemes. In collusion attack, two or more compromised nodes use an outside communication channel to coordinate an attack. For ECLDSSN, LEAP+ may be the most appropriate solution as SHELL and MUQAMI+ are designed for high density wireless sensor networks. For UESSN, Trusted Key Distribution Center (KDC) seems to be the most appropriate solution as it requires very little memory, which is the only concern in UESSN. However, it is not advisable to use Trusted KDC for a large-scale network because it creates bottleneck near the node trusted for key distribution. Public Key

Cryptography, coupled with an authentication service, can also be used if the target network is not a real-time network because computations of the Public Key Cryptography take longer time (in the order of seconds rather than milliseconds) on 8-bit processors. For real-time or large-scale UESSN, LEAP+ can be considered a better solution.

For LDDSN, Trusted Key Distribution Center (KDC) may be the most appropriate solution as it provides all security services. Public Key Cryptography, coupled with an authentication service also provides all security features and can also be used. For HDDSN, Public Key Cryptography coupled with an authentication service is the only solution, which provides all security features. However, if the computation costs of Public Key Cryptography are not bearable, then Polynomial Pool-based key Predistribution seems to be the most appropriate solution for HDDSN as it is the only solution, which offers more than just basic protection. For WBAN, BARI seems to be the most appropriate key management scheme as it is practical and specifically designed for WBAN scenario. Refer to Section 5 for quantitative comparison of various key management schemes in order to find out the most appropriate scheme for each scenario.

## 5. QUANTITATIVE COMPARISON

After discussing the key management schemes in Section 4, we indicated the most appropriate key management scheme for each scenario of wireless sensor networks. These indications are mainly dictated by the security services provided by each key management scheme, their applicability in each scenario and their apparent efficiency. However, for each wireless sensor network scenario it is important to quantify and compare the efficiency of all schemes, which are applicable and provide maximum security services in that scenario. In this regard, we performed simulations using Tools Command Langauge (tcl8.0), which is used to program ns-2 simulations.

In HDSSN, ECLDSSN and WBAN, every state-of-the-art key management scheme performs three tasks: initial deployment, key refreshment and node revocation. Key refreshment is the most important task as it is performed repeatedly. Initial deployment is performed only once and node revocation is just an occasional task. Therefore, we compare average energy consumed by a node each scheme during key refreshment task. For dynamic sensor networks (HDDSN and LDDSN), we assume that any two communicating nodes will have to establish keys from scratch. Therefore, we compare average energy consumed by a node in establishing a key from scratch. For UESSN, we compare memory consumption of the applicable schemes as energy is not a constraint in UESSN.

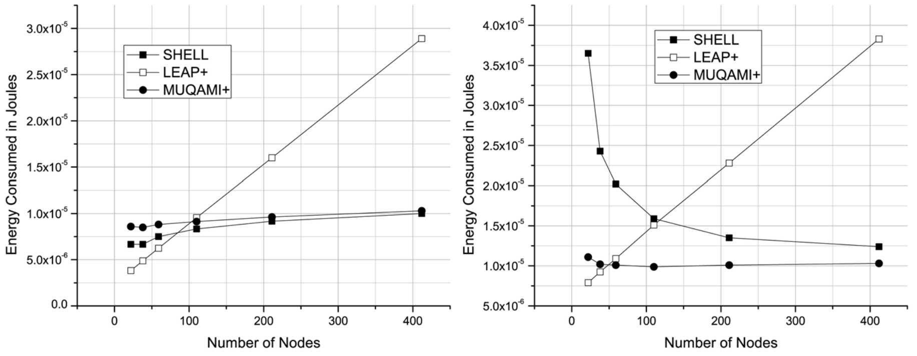
We have assumed that all sensor nodes are MICA2 motes, having ATMEGA128L CPU, and application level bandwidth of the wireless sensor network is 19.2 *kbps* [Karlof et al. 2004]. Some researchers [Xing et al. 2005] say that the application level bandwidth of wireless sensor networks is 6 *kbps*. We also performed simulations with application level bandwidth set to 6 *kbps* and found similar results. Power levels of the sensor nodes were set to be between –20 *dBm* and 10 *dBm* [Xing et al. 2005]. In all simulations, power level during reception phase and computation phase were assumed to be 0.1 *mW* (–10 *dBm*). For idle and sleep modes, we assumed the power levels of sensor nodes to be 0.01 *mW* (–20 *dBm*) and 0.006 *mW* (–22 *dBm*), respectively. Power level during transmission phase was set according to the distance between communicating nodes.

Further, we assume that IDEA cypher algorithm was used for encryption/ decryption, MD5 scheme was used for hashing and Elliptic Curve Cryptography (ECC) was used for Public Key Cryptography. For IDEA and MD5, we used the findings of [Venugopalan et al. 2003], which states that for 16 *bytes* on ATMEGA128L CPU, MD5 hashing scheme takes 1.45 *ms*, encryption using IDEA takes 0.68 *ms* and decryption using IDEA takes 2.42 *ms*. For ECC, we used the findings of [Wang and Li 2006], which states that 160-bit ECC signature generation and signature verification on MICA mote with ATMEGA128L CPU takes 1.3 *sec* and 2.8 *sec* respectively. Time required to generate random bytes on ATMEGA128L (8 MHz) CPU was dictated by the findings of [Seetharam and Rhee 2004]. In our simulations, we ensured that we record at least 30 occurrences of each event (for example, key refreshment) to avoid errors.

For HDSSN and ECLDSSN, we have compared the three state-of-the-art key management schemes (SHELL, LEAP+ and MUQAMI+). In this regard, we assumed clustered sensor networks and performed several simulation runs. In each simulation run, we varied node density in the network. The lowest number of nodes in a cluster was assumed to be 22 and the highest number of nodes in a cluster was assumed to be 412. In SHELL scheme, cluster heads need to communicate with the neighbouring cluster head nodes and SHELL and MUQAMI+ are based on EBS system of matrices. In this regard, we have assumed that the network has 5 clusters and values of EBS parameters are assumed to be between $k$+$m$=7 to $k$+$m$=12, depending on the cluster size. For SHELL, the number of neighbouring cluster head nodes, with which a cluster head node has to communicate, is set to 4. We assume that every sensor node has 10 neighbours on average and about half of them communicate with the cluster head node through it. Key-size was assumed to be 16-bytes and key-chain length for SHELL and MUQAMI+ was assumed to be 32.

For HDSSN and ECLDSSN, we assume clustered sensor networks, in which only cluster head node can communicate outside the cluster. In clustered sensor networks, a node within the same cluster is bound to be present in a smaller area around the transmitting node than a node that is outside the cluster. So, we have different power levels for inter-cluster and intra-cluster communications. Within intra-cluster communications, less transmission power is required if the receiving node is known to be a neighbour of the transmitting node. So, we assume different power levels for inter-cluster communication (10 *mW*), intra-cluster communication (1 *mW*) and communication between neighbouring nodes (0.1 *mW*). Underlying assumption for considering above power levels is that the distance between two cluster head nodes or a cluster head node and command node (base station) is about ten times the size of a cluster. Also, the maximum size of a cluster is about ten times the maximum distance between two neighbouring nodes.

In Figure 3, we compare average energy consumed by a node using each of the three schemes in static sensor networks. We varied the number of nodes in a cluster and then recorded the results. Figure 3(a) shows the result when energy consumed by



(a) Average energy consumed by a node (with cluster head node not included)

(b) Average energy consumed by a node (with cluster head node included)

Figure 3. Comparison of average energy consumed by a node using SHELL, LEAP+ and MUQAMI+ during key refreshment phase while varying the number of nodes in a cluster.

cluster head node is not included in the calculations. Figure 3(b) shows the result when energy consumed by cluster head node is included in the calculations. It is clear from these figures that LEAP+ is the best solution for ECLDSSN. As we increase the node density, performance of SHELL and MUQAMI+ increases and the performance of LEAP+ decreases. For HDSSN, if we don't have to consider the energy consumed by cluster head nodes, SHELL performs better than the other two schemes. Otherwise, it is clear that MUQAMI+ performs better than SHELL and LEAP+ for HDSSN.

For WBAN scenario, we compare BARI, LEAP+ and MUQAMI+. We did not choose to compare Plug'n Play key management because of its practical shortcomings. For example, it is nearly impossible for two nodes to record a reading at exactly the same time. For WBAN scenario, we consider that the network is a single cluster of 15 nodes and transmitting power level is always 1 $mW$ as all nodes directly communicate with the cluster head node (also known as the Personal Server). For MUQAMI+, we assumed EBS parameters $k$=$m$=4. All other simulation parameters were the same as that of ECLDSSN and HDSSN. Figure 4 compares the average energy consumed by a node for key refreshment using BARI, LEAP+ and MUQAMI+. Figure 4 also supports our intuition just like Figure 3. However, we find that MUQAMI+ performs better than LEAP+ even though this WBAN has a very small number of nodes. The reason for this discrepancy is that in WBAN scenario, all nodes are neighbours of each other and in LEAP+, more energy is consumed if the number of neighbours increase.

For dynamic sensor networks (HDDSN and LDDSN), we compare Trusted Key Distribution Center (KDC) and ECC based Public Key Cryptography, coupled with an authentication service. We kept the simulation parameters same and assumed that the trusted KDC is farthest from all sensor nodes i.e. nodes have to transmit at maximum power (10 $mW$) in order to communicate with it. In this case, we compare energy consumed by a node in order to establish a key with some other node. While keeping all other parameters constant we varied the transmitting power level of the nodes, which want to establish keys with each other because more transmission

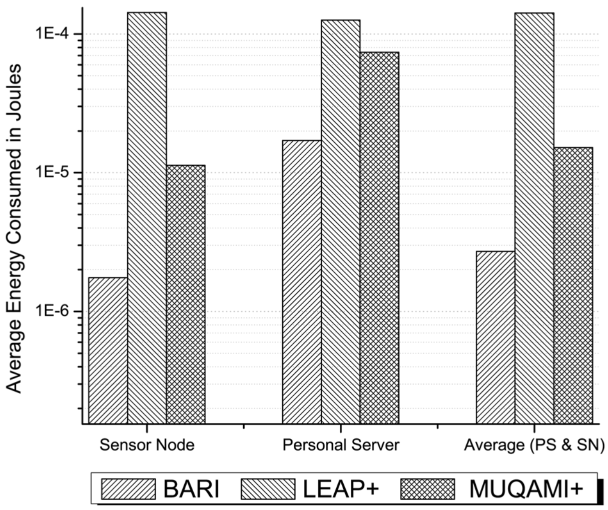


Figure 4. Average energy consumed by each type of node during key refreshment phase of WBAN scenario.

power is required if distance between nodes increases. Figure 5 compares Trusted KDC and ECC based public key cryptography. Even though a node has to communicate with the trusted KDC for every key establishment, it is lighter than Public Key Cryptography because of the computation costs involved. In order to achieve a key from Trusted KDC, each sensor node has to perform one encryption and one decryption, which takes 3.1 *ms* i.e. 0.31 *microJoules* while computations in Public Key Cryptography take 4.1 *seconds*, which amounts to 0.41 *milliJoules* per key exchange per node. Trusted KDC is the most appropriate choice for LDDSN. However, it

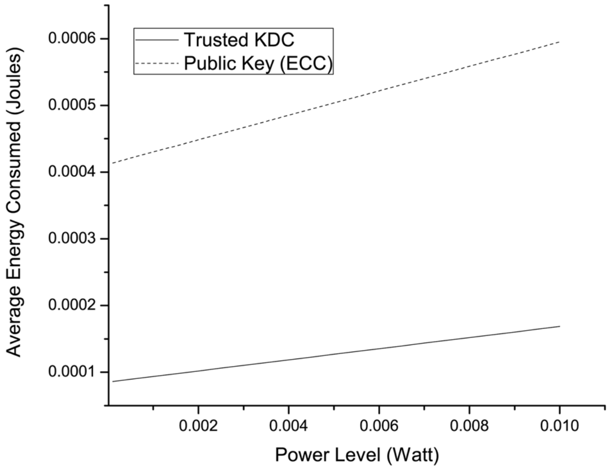
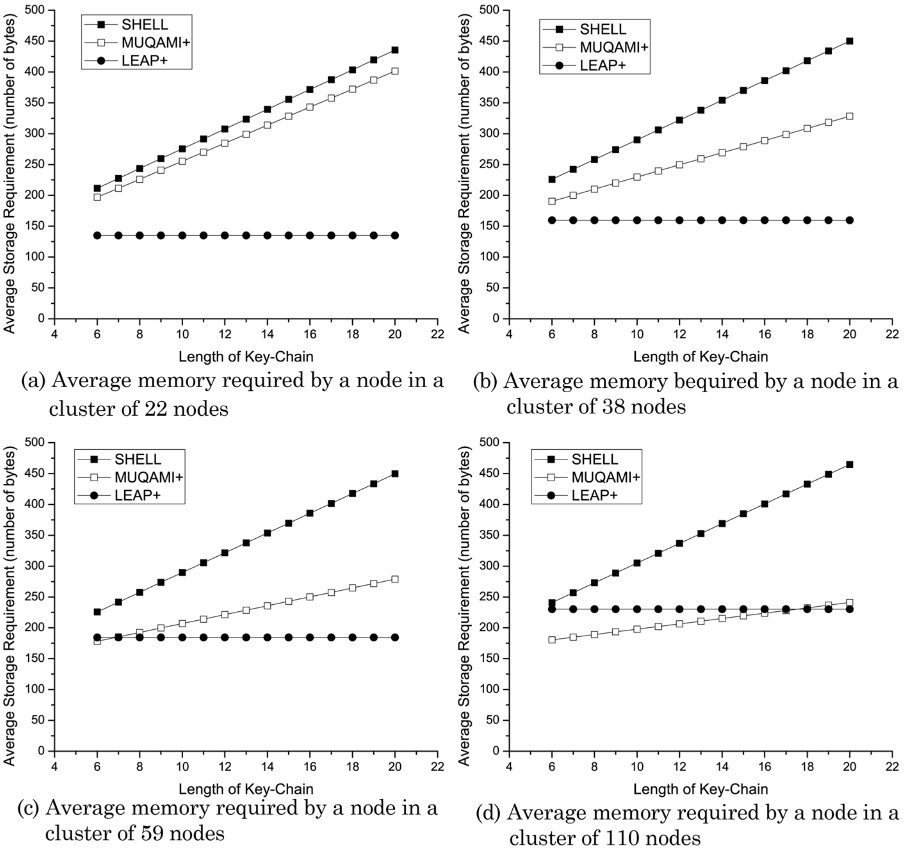


Figure 5. Average energy consumed by a sensor node in establishing a key using centralized key distribution center and ecc based public key cryptography while varying the transmission power level (transmission power level increases with the distance between nodes).

increases the traffic near the trusted KDC and becomes impractical for HDDSN. Therefore, ECC based Public Key Cryptography, coupled with an authentication service, is the only solution, which provides maximum security services for HDDSN.

We chose to show the results of UESSN in the end because this is the only case, in which we compare memory requirement rather than the energy consumption. If we use trusted KDC or ECC based Public Key Cryptography, coupled with an authentication service, then we don't need to store many keys in the sensor nodes. However, if we cannot use these schemes because of network size or other constraints, then we have to make a choice between other schemes. Therefore, we provide memory consumption analysis of SHELL, LEAP+ and MUQAMI+ in Figure 6. We did not compare with BARI because BARI is designed for networks, in which all nodes are in communication range of each other and it is not so in case of UESSN. Memory consumption of SHELL and MUQAMI+ depends upon the length of key-chains used while memory consumption of LEAP+ depends upon the number of neighbours each node has. So, we varied key-chain length and assumed different cluster size in each



(a) Average memory required by a node in a cluster of 22 nodes

(b) Average memory bequired by a node in a cluster of 38 nodes

(c) Average memory required by a node in a cluster of 59 nodes

(d) Average memory required by a node in a cluster of 110 nodes

Figure 6. Comparison of average storage requirement in a node using SHELL, LEAP+ and MUQAMI+ varying length of key-chain and node density in a cluster (high node density means higher number of neighbouring nodes).

of the sub-figures 6(a), 6(b) 6(c) and 6(d). We increased the number of neighbours with cluster size by assuming average number of neighbours to be square root of the total number of nodes in a cluster. In this case, average number of neighbours to a node was varied between 5 and 11. We can see that LEAP+ performs better than other schemes if average number of neighbours is less than 10.

## 6. CONCLUSIONS AND FUTURE WORK

There are many applications, for which sensor networks are deployed. It is important to identify different application areas so that researchers can focus on achieving efficient solutions for all types of sensor networks. We have identified wireless sensor network applications, classified sensor networks into different classes and identified security attacks that can take place in each class of sensor networks. In the end, we discussed prominent key management schemes for wireless sensor networks and their applicability in each class of wireless sensor networks. Also, we provided the quantitative comparison of the prominent key management schemes in each scenario.

Key Management schemes are important because they provide defence against attacks. However, it is equally important to research about attack detection mechanisms for wireless sensor networks. Our future research intends to explore attack detection mechanisms, suitable for each wireless sensor network scenario.

## ACKNOWLEDGMENTS

This research was supported by the MKE (Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the NIPA (National IT Industry Promotion Agency) (NIPA-2009-(C1090-0902-0002)). This work was also sponsored by the Basic Science Research Program funded by National Research Foundation (2009-0076798).

## REFERENCES

AKYILDIZ, I., W., SU, Y. SANKARASUBRAMANIAM, AND E. CAYIRCI. 2002. Wireless sensor net-works: A survey. *Computer Networks 38*, 4, 393–422.

AKYILDIZ, I. F., D. POMPILI, AND T. MELODIA. 2005. Underwater acoustic sensor networks: research challenges. *Ad Hoc Networks 3*, 3, 257–279.

AUGUSTO CELENTANO, S. F. AND PITTARELLO, F. 2009. The situation lens: A metaphor for personal task management on mobile devices. *Journal of Computing Science and Engineering 3*, 4 (December), 238–259.

BARGER, T., D. BROWN, AND M. ALWAN. 2005. Health-status monitoring through analysis of behavioral patterns. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on 35*, 1 (Jan.), 22–27.

BRAGINSKY, D. AND D. ESTRIN. 2002. Rumor routing algorthim for sensor networks. In *WSNA '02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications.* ACM, New York, NY, USA, 22–31.

CANTONI, V., L. LOMBARDI, AND P. LOMBARDI. 2007. Future scenarios of parallel computing: Distributed sensor networks. *Journal of Visual Languages & Computing 18*, 5, 484–491. In honour of Stefano Levialdi.

CHAKRABARTY, K., S. S. IYENGAR, H. QI, AND E. CHO. 2002. Grid coverage for surveillance and target location in distributed sensor networks. *IEEE Transactions on Computers 51*, 12, 1448–1453.

CHAN, H., A. PERRIG, AND D. SONG. 2003. Random key predistribution schemes for sensor networks. In *SP '03: Proceedings of the 2003 IEEE Symposium on Security and Privacy.*

IEEE Computer Society, Washington, DC, USA, 197.

Cherukuri, S., K. K. Venkatasubramanian, and E. K. S. Gupta. 2003. BioSec: A biometric based approach for securing communication. In *in Wireless Networks of Biosensors Implanted in the Human Body, Workshop on Wireless Security and Privacy (WiSPr), International Conference on Parallel Processing Workshops, 2003.*

Clarkson, B., A. Pentland, and K. Mase. 2000. Recognizing user context via wearable sensors. *Wearable Computers, IEEE International Symposium 0*, 69.

Cook, D. J., M. Youngblood, III, E. O. Heierman, K. Gopalratnam, S. Rao, A. Litvin, and F. Khawaja. 2003. Mavhome: An agent-based smart home. In *PERCOM '03: Proceedings of the First IEEE International Conference on Pervasive Computing and Communications*. IEEE Computer Society, Washington, DC, USA, 521.

Dierks, T. and C. Allen. 1999. The tls protocol version 1.0.

Diffie, W. and M. E. Hellman. 1976. New directions in cryptography. *IEEE Transactions on Information Theory IT-22*, 6, 644-654.

Dini, G. and I. M. Savino. 2006. An efficient key revocation protocol for wireless sensor networks. In *WOWMOM '06: Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*. IEEE Computer Society, Washington, DC, USA, 450–452.

Eltoweissy, M., M. H. Heydari, L. Morales, and I. H. Sudborough. 2004. Combinatorial optimization of group key management. *J. Netw. Syst. Manage. 12*, 1, 33–50.

Eschenauer, L. and V. D. Gligor. 2002. A key-management scheme for distributed sensor networks. In *CCS '02: Proceedings of the 9th ACM conference on Computer and communications security*. ACM, New York, NY, USA, 41–47.

Estrin, D., R. Govindan, J. Heidemann, and S. Kumar. 1999. Next century challenges: scalable coordination in sensor networks. In *MobiCom '99: Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*. ACM, New York, NY, USA, 263–270.

Falck, T., H. Baldus, J. Espina, and K. Klabunde. 2007. Plug'n play simplicity for wireless medical body sensors. *Mob. Netw. Appl. 12*, 2-3, 143–153.

Ghumman, K. 2006. Location-aware combinatorial key management scheme for clustered sensor networks. *IEEE Trans. Parallel Distrib. Syst. 17*, 8, 865–882. Senior Member-Mohamed F. Younis and Senior Member-Mohamed Eltoweissy.

Gui, C. and P. Mohapatra. 2004. Power conservation and quality of surveillance in target tracking sensor networks. In *MobiCom '04: Proceedings of the 10th annual international conference on Mobile computing and networking*. ACM, New York, NY, USA, 129–143.

Gura, N., A. Patel, A. W, H. EBerle, and S. C. Shantz. 2004. Comparing elliptic curve cryptography and rsa on 8-bit cpus. 119–132.

Gyselinckx, B., C. van Hoof, J. Ryckaert, R. Yazicioglu, P. Fiorini, and V. Leonov. 2005. Human++: autonomous wireless sensors for body area networks. In *Custom Integrated Circuits Conference, 2005. Proceedings of the IEEE 2005*. 13–19.

He, T., S. Krishnamurthy, L. Luo, T. Yan, L. Gu, R. Stoleru, G. Zhou, Q. Cao, P. Vicaire, Stankovic, J. A., Abdelzaher, T. F., Hui, J., and Krogh, B. 2006. Vigilnet: An integrated sensor network system for energy-efficient surveillance. *ACM Trans. Sen. Netw. 2*, 1, 1–38.

He, T., S. Krishnamurthy, J. A. Stankovic, T. Abdelzaher, L. Luo, R. Stoleru, T. Yan, L. Gu, J. Hui, and B. Krogh. 2004. Energy-efficient surveillance system using wireless sensor networks. In *MobiSys '04: Proceedings of the 2nd international conference on Mobile systems, applications, and services*. ACM, New York, NY, USA, 270–283.

Holman, R., J. Stanley, and T. Ozkan-Haller. 2003. Applying video sensor networks to nearshore environment monitoring. *Pervasive Computing, IEEE 2*, 4 (Oct.-Dec.), 14–21.

Huang, Q., J. Cukier, H. Kobayashi, B. Liu, and J. Zhang. 2003. Fast authenticated key establishment protocols for self-organizing sensor networks. In *WSNA '03: Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications*. ACM, New York, NY, USA, 141–150.

INTILLE, S. S. 2002. Designing a home of the future. *IEEE Pervasive Computing 1*, 2, 76–82.

JOVANOV, E., A. MILENKOVIC, C. OTTO, AND P. DE GROEN. 2005. A wireless body area net-work of intelligent motion sensors for computer assisted physical rehabilitation. *Journal of Neuro Engineering and Rehabilitation 2*, 1, 6.

KARLOF, C., Y. LI, AND J. POLASTRE. 2003. Arrive: an architecture for robust routing in volatile environments. Tech. Rep. CSD-03-1233, University of California at Berkeley.

KARLOF, C., N. SASTRY, AND D. WAGNER. 2004. TinySec: a link layer security architecture for wireless sensor networks. In *SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems*. ACM, New York, NY, USA, 162–175.

KLEMM, M. AND G. TROESTER. 2006. Textile uwb antennas for wireless body area networks. *Antennas and Propagation, IEEE Transactions on 54*, 11 (Nov.), 3192–3197.

KOHL, J. AND C. NEUMAN. 1993. The kerberos network authentication service (v5).

LAMPORT, L. 1981. Password authentication with insecure communication. *Commun. ACM 24*, 11, 770–772.

LIU, D. AND P. NING. 2003. Establishing pairwise keys in distributed sensor networks. In *CCS '03: Proceedings of the 10th ACM conference on Computer and communications security.* ACM, New York, NY, USA, 52–61.

MADDEN, S., R. SZEWCZYK, M. J. FRANKLIN, AND D. CULLER. 2002. Supporting aggregate queries over ad-hoc wireless sensor networks. In *WMCSA '02: Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications.* IEEE Computer Society, Washington, DC, USA, 49.

MAINWARING, A., D. CULLER, J. POLASTRE, R. SZEWCZYK, AND J. ANDERSON. 2002. Wireless sensor networks for habitat monitoring. In *WSNA '02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications.* ACM, New York, NY, USA, 88-97.

MALAN, D., M. WELSH, AND M. SMITH. 2004. A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography. In *Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference on.* 71–80.

MARTINEZ, K., J. K. HART, AND R. ONG. 2004. Environmental sensor networks. *Computer 37*, 8, 50–56.

NILSSON, D. K., T. ROOSTA, U. LINDQVIST, AND A. VALDES. 2008. Key management and secure software updates in wireless process control environments. In *WiSec '08: Proceedings of the first ACM conference on Wireless network security.* ACM, New York, NY, USA, 100–108.

NOURY, N., T. HERVE, V. RIALLE, G. VIRONE, E. MERCIER, G. MOREY, A. MORO, AND T. PORCHERON. 2000. Monitoring behavior in home using a smart fall sensor and position sensors. In *Micro-technologies in Medicine and Biology, 1st Annual International, Conference On. 2000.* 607–610.

OTTO, C., A. MILENKOVIC, C. SANDERS, AND E. JOVANOV. 2006. System architecture of a wireless body area sensor network for ubiquitous health monitoring. *Journal of Mobile Multimedia 1*, 4, 307–326.

POON, C., Y. ZHANG, AND S. BAO. 2006. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communication Magazine 44*, 4, 73–81.

RAAZI, S. M. K., H. LEE, S. LEE, AND Y.-K. LEE. 2009a. BARI: A distributed key management approach for wireless body area networks. In 2009 *International Conference on Computational Intelligence and Security (CIS 2009).* Beijing, China.

RAAZI, S. M. K., H. LEE, S. LEE, AND Y.-K. LEE. 2009b. MUQAMI+: a scalable and locally distributed key management scheme for clustered sensor networks. *Annals of Telecommunications.*

RIVEST, R., A. SHAMIR, AND L. ADLEMAN. 1978. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM 21*, 120–126.

RUAIR, R. M., M. T. KEANE, AND G. COLEMAN. 2008. A wireless sensor network application requirements taxonomy. *Sensor Technologies and Applications, International Conference on 0*, 209–216.

SEETHARAM, D. AND S. RHEE. 2004. An efficient pseudo random number generator for low-power sensor networks. In *LCN '04: Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks*. IEEE Computer Society, Washington, DC, USA, 560–562.

TILAK, S., N. ABU-GHAZALEH, AND HEINZELMAN, W. 2002. A taxonomy of wireless microsensor network models. *ACM Mobile Computing and Comm. 6*, 2, 1–8.

TIMMONS, N. AND W. SCANLON. 2004. Analysis of the performance of ieee 802.15.4 for medical sensor body area networking. In *Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference on*. 16–24.

VENUGOPALAN, R., P. GANESAN, P. PEDDABACHAGARI, A. DEAN, F. MUELLER, AND M. SICHITIU. 2003. Encryption overhead in embedded systems and sensor network nodes: modeling and analysis. In *CASES '03: Proceedings of the 2003 international conference on Compilers, architecture and synthesis for embedded systems*. ACM, New York, NY, USA, 188–197.

WANDER, A. S., N. GURA, H. EBERLE, V. GUPTA, AND S. C. SHANTZ. 2005. Energy analysis of public-key cryptography for wireless sensor networks. In *PERCOM '05: Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications*. IEEE Computer Society, Washington, DC, USA, 324–328.

WANG, H. AND Q. LI. 2006. Efficient implementation of public key cryptosystems on mote sensors (short paper. In *In International Conference on Information and Communication Security (ICICS), LNCS 4307*. 519–528.

WARD, A., A. JONES, AND A. HOPPER. 1997. A new location technique for the active office. *Personal Communications, IEEE 4*, 5 (Oct), 42–47.

XIAO, Y., V. K. RAYI, B. SUN, X. DU, F. HU, AND M. GALLOWAY. 2007. A survey of key management schemes in wireless sensor networks. *Computer Communications 30*, 11-12, 2314–2341. Special issue on security on wireless ad hoc and sensor networks.

XING, G., C. LU, Y. ZHANG, Q. HUANG, AND R. PLESS. 2005. Minimum power configuration in wireless sensor networks. In *MobiHoc '05: Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*. ACM, New York, NY, USA, 390–401.

XU, N. 2002. A survey of sensor network applications. *IEEE Communications Magazine 40*.

YAN, T., T. HE, AND J. A. STANKOVIC. 2003. Diffierentiated surveillance for sensor networks. In *SenSys '03: Proceedings of the 1st international conference on Embedded networked sensor systems*. ACM, New York, NY, USA, 51–62.

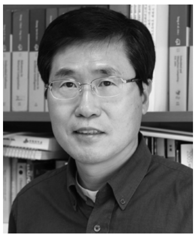
YOO, I. AND SONG, M. 2008. Biomedical ontologies and text mining for biomedicine and healthcare: A survey. *Journal of Computing Science and Engineering 2*, 2 (June), 109–136.

ZASOWSKI, T., F. ALTHAUS, M. STAGER, A. WITTNEBEN, AND G. TROSTER. 2003. Uwb for noninvasive wireless body area networks: channel measurements and results. In *Ultra Wideband Systems and Technologies, 2003 IEEE Conference on*. 285–289.

ZHU, S., S. SETIA, AND S. JAJODIA. 2006. LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. *ACM Trans. Sen. Netw. 2*, 4, 500–528.

ZIA, T. AND A. ZOMAYA. 2006. Security issues in wireless sensor networks. In *Systems and Networks Communications, 2006. ICSNC '06. International Conference on*. 40–40.

**Syed Muhammad Khaliq-ur-Rahman Raazi** received his B.S. degree in Computer Software Engineering from National University of Sciences and Technology (NUST), Rawalpindi, Pakistan in 2002. He got his MS degree from Lahore University of Management Sciences (LUMS), Lahore, Pakistan in 2006. He also has more than two years industry experience as System & Software Engineer Engineer. Currently, he is a Ph.D. candidate in the Dept. of Comp. Eng., Kyung Hee University (Global Campus), South Korea. His research interests include Security, Key management, Ubiquitous computing, Wireless Sensor Networks, Ubiquitous Health Care, Cloud Computing.



**Sungyoung Lee** received his B.S. from Korea University, Seoul, Korea. He got his M.S. and PhD degrees in Computer Science from Illinois Institute of Technology (IIT), Chicago, Illinois, USA in 1987 and 1991 respectively. He has been a professor in the Dept. of Computer Engineering, Kyung Hee University, Korea since 1993. He is a founding director of the Ubiquitous Computing Laboratory, and has been affiliated with a director of Neo Medical ubiquitous- Life Care Information Technology Research Center, Kyung Hee University since 2006. Before joining Kyung Hee University, he was an assistant professor in the Dept. of Comp. Sci., Governors State University, Illinois, USA from 1992 to 1993. His current research focuses on Ubiquitous Computing and applications, Context-aware Middleware, Sensor Operating Systems, Real-Time Systems and Embedded Systems. He is a member of the ACM and IEEE.