Author(s): Chow, C. ; Ishii, H. ; Kocher, I. ; Zia, T.A.

Title: Threat Models and Security Issues in Wireless Sensor Networks

Conference: International Conference on Intelligent Network and Computing (ICINC)

Location: Kuala Lumpur, Malaysia **Date:** 26-28 November 2010

Year: 2010 **Pages:** VI384 - 389

Editor: Zhang Yushu

Publisher: IACSIT

Place of Publication: Chengdu, China

Abstract: Security is a crucial issue for wireless sensor networks due to the deployment nature and the resources limitations of tiny sensor devices used in such networks. Sensor networks are used sometime in very sensitive applications such as healthcare and military. With this in mind we must address the security concerns from the beginning of network design. Owing to limited resources and computing constraints security in sensor networks poses more severe challenges as compare to the traditional networ ...

Threat Models and Security Issues in Wireless Sensor Networks

Idrees S Kocher
Dept. of Electrical Engineering
University of Malaya , UM
Kuala Lumpur , Malaysia
husseinidrees@yahoo.com

Chee-Onn Chow
Dept. of Electrical Engineering
University of Malaya , UM
Kuala Lumpur , Malaysia
cochow@um.edu.my

Hiroshi Ishii
Professional Graduate School of Embedded Technology
Tokai University
Hiratsuka , Japan
ishii@dt.u-tokai.ac.jp

Tanveer A Zia
School of Computing and Mathematics
Charles Sturt University
NSW, Australia
tzia@csu.edu.au

Abstract— **Security is a crucial issue for wireless sensor networks due to the deployment nature and the resources limitations of tiny sensor devices used in such networks. Sensor networks are used sometime in very sensitive applications such as healthcare and military. With this in mind we must address the security concerns from the beginning of network design. Owing to limited resources and computing constraints security in sensor networks poses more severe challenges as compare to the traditional networks. There are currently enormous approaches in the field of wireless sensor networks security. No comprehensive study lists the security issues and the threat models which pose unique threats to the wireless sensor networks. In this paper we have corroborated well known security issues and have provided the direction of research towards effective countermeasures against the threats posed by these issues.**

Keywords: Threat models; wireless sensor networks; security issues; network aattacks; countermeasures.

I. INTRODUCTION

We envision in near future that hundreds to thousands of sensor devices will be used in self-organizing wireless sensor networks (WSNs). Indeed wireless sensor networks gaining rapid popularity because of their potentially low cost solutions to a variety of real-world challenges [1] . Security in WSNs is not easy; compared with conventional desktop computers, severe challenges meet these sensor nodes, such as limitation in processing power, storage, channel bandwidth and energy. We attempt to overcome these challenges, due to importance of security. Sensor networks have the potential to be deployed in applications in all aspects of our lives. Some typical applications are energy management, logistics and inventory management, battlefield and emergency response information. Sensor networks pose unique security challenges because of their inherent limitations in communication and computing abilities.

Deployment of sensor networks in an unattended environment makes them vulnerable to potential attacks. Attackers can compromise the network to accept malicious nodes as legitimate nodes. Hardware and software improvements will address these issues at some extend but comprehensive security requires development of countermeasures such as secure key management, lightweight encryption techniques, secure routing protocols and malicious node detection mechanism. This paper provides an overview of security issues and threat models in WSNs and provides direction for research in developing the countermeasures.

The rest of the paper is organized as follows. In Section II we summarize the obstacles for the sensor network security. In Section III the requirements of a wireless sensor network security are listed. The major attacks in sensor network are categorized in Section IV, and we outline the corresponding defensive measures in Section V. Finally, section VI points out our future observation and concludes the paper.

II. OBSTACLES FOR WIRELESS SENSOR SECURITY

A wireless sensor network has many constraints compared to other networks, because of these constraints it is more difficult to directly deploy the traditional security approaches in WSNs . Therefore, to develop useful security mechanisms while borrowing the ideas from the existing security techniques, it is impressive to understand these constraints first as in [2].

A. Limited Resources

All security techniques require a specific amount of resources for the implementation, including code space, data memory, and energy to power the sensor devices. However, these resources are very limited in a wireless sensor device. The two major limitations are storage space and battery power:

- Limited Storage Space and Memory: A tiny sensor device has a small amount of memory and storage space for the code. Indeed, to construct effective security techniques, it is necessary to limit the size of the security algorithm cod. For example, Zigbex sensor type (HBE) has an 8-bit, 7.372 MHz ATmega128L RISC MCU with only 4Kb SRAM, 128 Kb flash memories, and 512Kb flash storage [33].
- Power Limitation: Another strongest constraint to wireless sensor capabilities is power energy. Once sensor nodes are deployed in a sensor network the energy must be conserved for prolonging the life of the individual sensor node and the entire sensor network.

B. Unreliable Communication

The secure network depends on a protocol, which eventually, depends on communication within the entire network.

- Unreliable Transfer: Because of the inherent unreliable wireless routing in sensor network, packets may get damaged due to channel errors or dropped at highly congested nodes in the network.
- Conflicts: Due to the broadcast nature of the wireless sensor network, packets may collide in the middle of transfer and conflict will occur .
- Latency: Latency is due to the multi-hop routing, congestion, and node processing delay in the sensor network. In the presence of latency it is too difficult to achieve synchronization among sensor nodes.

C. Unattended Operation

The inherent unattended deployment nature of WSNs in an environment is open to adversaries attack and natural disasters such as bad weather and bushfires. Therefore, sensor nodes suffer physical attacks in such an environment.

III. SECURITY REQUIREMENTS FOR WSNS

In this section, we present a brief overview for a security goals in sensor networks .Requirements of WSNs are encompassing both the typical network requirements and the unique requirements suited solely to WSNs.

A. Data Confidentiality

It is the ability to hide message from a passive attacker and is the most important issue in network security. The network with any security focus must address this problem. In sensor networks, the confidentiality relates to the following:

- A sensor network should not leak sensor readings to its neighbors.
- Sensor nodes may communicate highly sensitive data, such as key distribution, so it is extremely important to build a secure channel in a wireless sensor network.
- Sensor identities and public keys should also be encrypted to some extent to protect against traffic analysis attack.

B. Data Integrity and Athentication

Integrity refers to the ability to confirm the message has not been tampered or changed while it was on the network.

An adversary is not just limited to modifying the data packet. It can change the whole packet stream by injecting additional packets. So the receiver needs to ensure that the data used in any decision-making process originates from the correct source. Indeed, data authentication allows a receiver to verify that the data really is sent by the claimed sender. In the case of two-party communication, data authentication can be achieved through a purely symmetric mechanism.

C. Data Freshness

By supposing that both forenamed goals are assured, we also need to ensure the freshness of each message. Informally, data freshness suggests that the data are recent, and it ensures that no messages have been replayed. This requirement is especially important when there are shared-key strategies employed in the design and need to be changed over time.

D. Availability

It is to verify if a node has the ability to utilize the resources and the network is available for the message to move on.

E. Self-Organization

WSN is typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature also brings a great challenge to wireless sensor network security.

F. Time Synchronization

Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor's radio may be turned off for periods of time. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two sensors. A more collaborative sensor network may require group synchronization for tracking application.

G. Secure Localization

The use of a sensor network will depend on its ability to accurately and automatically locate each node in the network. A sensor network designed to locate faults, this need accurate location information in order to pinpoint the location of a fault.

IV. ATTACKS ON SENSOR NETWORKS

Wireless sensor networks are not limited to simply denial of service attacks, but rather encompass a variety of techniques including node takeovers, attacks on the routing protocols, and

Ministry of Higher Education and Scientific Research , Scholarship Program, Erbil, Iraq .
UM.TNC2/IPPP/UPGP/Grant(PPP)PS134/2010A.

attacks on a node's physical security. In this section, we first address some common denial of service attacks [5].

A. *Types of Denial of Service attacks*

The transmission of a radio signal that interferes with the radio frequencies being used by the sensor network is called jamming[6].Jamming may come in two forms: constant jamming, and intermittent jamming. Constant jamming implies the jamming of the entire network. While in the case of intermittent jamming, the sensor nodes are able to exchange messages periodically.

At the link layer, one possibility is that an attacker may simply intentionally violate the communication protocol, e.g., ZigBee [3] or IEEE 802.11b protocol, and continually transmit messages in an attempt to generate collisions. Such collisions would require the retransmission of any packet lost by the collision.

At the routing layer, a node may take advantage of a multi-hop network by simply refusing to route messages. With the net result being that any neighbor who routes through the malicious node will be unable to exchange messages with the part of the network.

The transport layer is also vulnerable to attack, as in the case of flooding. Flooding means sending many connection requests to a malicious node. In this case, resources must be allocated to handle the connection request. Eventually a node's resources will be exhausted, thus rendering the node useless.

B. *The Sybil attack*

Reference [7] defines Sybil attack as a malicious node illegitimately taking on multiple identities. It was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks .

C. *Traffic Analysis Attacks*

Often, for an attacker to effectively render the network in useless state, the attacker can simply disable the base station. To make matters worse, Authors in[8]demonstrate two attacks that can identify the base station in a network without even understanding the contents of the packets. A rate monitoring attack posits that nodes close to the base station tend to forward more packets than those farther away from the base station. While in a time correlation attack, an attacker generates events and monitors to whom a node sends its packets.

D. *Node Replication Attacks*

By copying the node ID of an existing node an attacker can add a node to an existing sensor network. A replicated node can severely disrupt a sensor network's performance, packets can be corrupted or even misrouted. This can result in a disconnected network and false sensor readings [9].

E. *Physical Attacks*

Indeed, in hostile outdoor environments, the small form factor of the nodes, coupled with the unattended and distributed nature of their deployment makes them vulnerable to physical attacks [10].Physical attacks ruin sensors permanently, so the losses are irreversible. For instance, attackers can access cryptographic secrets, tamper with the associated circuitry, spoofing /modifying programming in the nodes, and /or replace them with malicious nodes all of these within the control of the attacker.

V. DEFENSIVE MEASURES IN SENSOR NETWORKS

This section describes the countermeasures for satisfying the security requirements and protecting the sensor network from attacks. Table 1 below summarizes the attacks and countermeasures in a layering model in WSNs [11].

TABLE I. LAYERING APPROACH IN SENSOR NETWORK ATTACKS AND COUNTERMEASURES

Layers	Attack types	Countermeasures
Application Layer	Subversion and Malicious Nodes	Malicious Node Detection and Isolation
Network Layer	Sinkholes, wormholes, Sybil,Routing Loop	Key Management, Secure Routing
Data Link Layer	Link Layer Jamming	Link Layer encryption
Physical Layer	DOS and Node capture attacks	Adaptive antennas, Spread Spectrum

A. *Defending Against DoS Attacks*

One strategy in defending against the jamming attack is to identify the jammed part of the sensor network and effectively route around the unavailable portion.

To handle jamming at the MAC layer, nodes might utilize a MAC admission control that is rate limiting. This would allow the network to ignore those requests designed to exhaust the power reserves of a node. This, however, is not fool-proof as the network must be able to handle any legitimately large traffic volumes.

To overcome the transport layer flooding denial of service attacks, reference [12] suggests using the client puzzles in an effort to discern a node's commitment to make the connection by utilizing some of their own resources.

Current Denial-of-service (DoS) attacks are targeted towards a specific victim ,in contrast a Coremelt attack, which is a new attack technique, where attackers only establish traffic between each other, and not towards a victim host. To the best of our knowledge the best solution to DoS attacks is to utilize puzzles to increase the cost for attacker to consume victim resources. If the amount of work required to complete the puzzle is large enough, the attacker will no longer be able to launch a successful attack [13].

B. *Defending Against Attacks on Routing Protocols*

There is a great need for both secure and energy efficient routing protocols in WSNs against attacks such as the sinkhole, wormhole and Sybil attacks [7,14].

Authors in [15]describe an intrusion tolerant routing protocol , INSENS, which is designed to limit the scope of an

intruder ruining and rout information within network intrusion. They posit utilizing the base station to compute routing tables on behalf of the individual sensor nodes. This is done in three phases. The forwarding tables will include the redundancy information used for the redundant message transmission. Attacks that can be made on the routing protocol during each of the three phases above are: First, sensor node might fool the base station by sending a bogus request message. Second ,a compromised node might also include a bogus path(s) when forwarding the requested message to its neighbors. Finally, it may not even forward the requested message at all. The defense to overcome these issues, they use a scheme similar to µTESLA where one- key chains are used to identify a message originating from the base station.

Reference [16] describes TRANS routing protocol. This protocol is designed for utilizing in data centric networks. The authors make use of a loose-time synchronization asymmetric cryptographic scheme to ensure confidentiality of message. They also use µTESLA in their implementation which is used to ensure message authentication and confidentiality.

To the best of our knowledge, the concept of wormholes in a sensor network is still effective threat. This attack is one in which a compromised node eavesdrops on a series of packets, tunnels them via the sensor network to another compromised node, and then replays the packets. Indeed, this can be done to misrepresent the distance between the two colluding nodes. It can also be used to more generally disrupt the routing protocol by misleading the neighbor discovery process. So far all existing solutions no longer overcome this attack.

To counter against the Sybil attack described previously in Section IV.B, we need a mechanism to assure that a particular identity is the only one being held by a given physical node. Reference [7] presents two methods to assure identities, indirect validation and direct validation. In indirect validation, a third party trusted node is allowed to witness for (or against) the validity of a joining node. While in direct validation a trusted node directly witnesses whether the joining identity is valid. Direct validation techniques, including a radio resource test. In this test, a sensor node assigns each of its neighbors a different channel on which to communicate. The node then randomly checks a channel and listens. If there is a transmission on the channel it is assumed that the node transmitting on the channel is a physical node otherwise not a physical identity.

C. Combating Traffic Analysis Attacks

Authors in [8] use a random walk forwarding mechanism that occasionally forwards a packet to a node other than the sensor's parent node. This would make it difficult to discern a clear path from the sender node to the base station (BS) and would help to mitigate the rate monitoring attack, but would still be susceptible to the time correlation attack. To strive against the time correlation attack, it suggests a fractal propagation strategy. In this mechanism a node will generate a forged packet when its neighbor is forwarding a packet to the base station. The forged packet is sent randomly to another neighbor who may also generate a forged packet. These packets essentially use a time-to-live to decide when the packet should discard. This effectively hides BS from time correlation attacks.

D. Key Management and Protocols

Sensor nodes may be deployed in a hostile environment; however, security becomes extremely important, as they are prone to variant types of malicious attacks. The open problem is how to set up pair-wise secret key between communicating nodes. In one of the recently presented secure schemes [17], the authors describe security as important as performance and energy efficiency for many applications. Key pre-distribution is a good idea to solve the key agreement problems in wireless sensor network, but in this case, the attacker might reveals it after compromising the node. Based on the Key-Insulated Encryption KIE-WSNs, authors have proposed a new key pre-distribution scheme. They achieved both semantically security and optimal KIE-(N-1,N)safety, which means that even if N-1 nodes are compromised, there are no security threat to the remaining network.

Key ring distribution mechanism in each node is described by [18]. The key ring consists of a number of randomly chosen keys from a much larger pool of keys generated offline.

Reference [19] posits that the single security requirement is not precisely fits all types of communication in a wireless sensor network. With this in mind, set of four different keys are proposed depending on whom the node is communicating with. The initial key is preloaded to each sensor node and further keys can be established from it later. We propose that the initial key should be deleted after its use to avoid the network from additional compromised nodes once there is a compromised sensor in network .

Authors in [20] address a scheme for establishing a key between two nodes that is based on the common trust of a third node anywhere within the sensor network. The nodes and their shared keys are spread over the network such that for any two nodes A and B, there is a node C that shares a key with both A and B. Therefore, the key establishment protocol between A and B can be securely routed through C. From a security precaution, a node C's trust should be verified.

Reference [21] posits that an individual node possesses far less computational power and energy than a base station. They posit the major cryptographic burden on the base station with a greater resource. On the node side,elliptic curve cryptography is often used in sensors due to the fact that relatively small key sizes are required to provide an expected level of security. In addition, this technique also utilizes certificates to establish the lawfulness of a public key. The certificates are based on an elliptic curve implicit certificate technique .We strongly recommend that such certificates are useful to verify the lawfulness of the nodes before joining the network.

Recently many papers have outlined that it may be possible to utilize radio finger-printing to identify the origin of messages in sensor network [22]. It is easy to use such mechanisms to create a list of sensor nodes that are authorized members of the network, thereby noticing the presence of the attacker's devices.

Authors in [30] describe more energy efficient pair wise key establishment scheme. The nodes set up its own keys through the communication with their neighboring nodes. The key idea is to divide the network into levels and sectors to limit neighborhood of a particular node. The authors have proved in simulation tests that the protocol has advantages in terms of energy and storage over existing approaches.

We envision that successful protocol for key establishment in wireless sensor network, must own feature of establishing new keys without requiring any secret values in both participating nodes, thereby, passive or active attacking nodes can't perform MitM (Man-in-the-Middle)attacks, as long as the attacker is remote and no longer will be able to insert its own computationally more powerful nodes into the network [23].

E. Secure Broadcasting and Multicasting

The major communication pattern of wireless sensor networks is broadcasting and multicasting, e.g., 1-to-Y, Y-to-1, and X-to-Y, in contrast to the traditional point-to-point communication on the Internet network. In the following subsections we describe secure multicasting and broadcasting patterns:

- Secure Multicasting Pattern: Reference [24] proposes a directed diffusion based multicast technique for wireless sensor networks considering also the advantage of a logical key hierarchy . The key distribution center, is the root of the key hierarchy while individual sensor nodes make up the leaves. By utilizing this technique, they modify the logical key hierarchy to build a directed diffusion based logical key hierarchy. This technique provides mechanisms for sensor nodes joining and leaving groups where the key hierarchy is used to effectively re-key all nodes within the leaving node's hierarchy.
- Secure Broadcasting Pattern: Reference [25] suggests a routing-aware based tree where the leaf nodes are assigned keys based on all relay nodes above them. This technique takes advantage of routing information and is more energy efficient than mechanisms that arbitrarily arrange sensor nodes into the routing tree.

Authors in[26]describe mechanism which takes advantage of geographic location information (GPS) instead of routing information. Sensor nodes are grouped into clusters with the observation that nodes within a cluster will be able to reach one another within a single hop. Indeed, by using the cluster information, a key hierarchy is constructed as in [25].

F. The Malicious Nodes Monitoring Mechanism forWSNs

Reference [27] describes the function of this mechanism. Node A is a monitoring node sends a message to Node D, and monitors the behavior of Node D. Figure 1 shows a message sent by Node A, secured with the network key Kn while in figure 2 shows an altered message from Node D. We envision, this mechanism prevents or mitigates most of the well known routing attacks such as sinkholes ,selective forwarding, wormholes, and Sybil attacks. Utilizing a monitoring mechanism to detect suspicious behavior, and on the basis of the responses from other monitoring nodes, if the number of suspicious entries concerning a particular node reaches a set threshold, that node is declared malicious. Alarming all the neighbors and eventually reaching the base station. The base station isolates the malicious node and all traffic coming from that node is discarded.

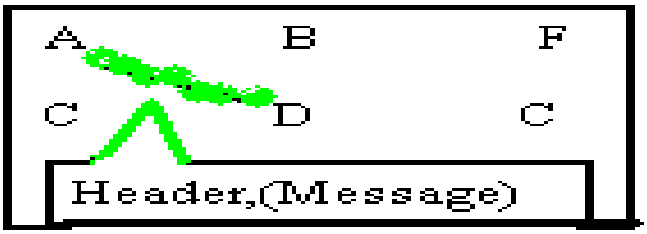

Figure 1. Message sent by Node A

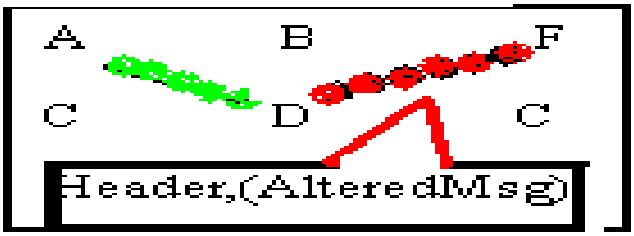

Figure 2. Message altered by Node D

G. Complete Security Framework for WSNs

An integrated holistic security framework that will provides security services of WSNs is proposed in [31]. The authors have added one extra module i.e. Intelligent Security Agent (ISA) to assess level of security and cross layer interaction. This comprehensive framework comprises of many components, as such Intrusion Detection System, Trust Framework , key management Scheme and Link Layer Communication Protocol. The overhead added by this technique is related to the level of security which in turn relied on underlying application.

However, to the best of our knowledge, most of the existing security approaches for WSNs are layer wise i.e. a particular solution is applicable to single layer itself. So, to integrate them all is a new research challenge.

VI. CONCLUSIONS

Wireless sensor networks have become promising future to many applications. In the absence of adequate security, deployment of sensor networks is vulnerable to variety of attacks. In this paper we have outlined the four main aspects of wireless sensor network security: obstacles, requirements, attacks, and defenses. Within each of those categories we have

also sub-categorized the major topics including routing, trust, denial of service, and so on. Our aim is to provide a general overview of the rather broad area of wireless sensor network, security issues, threat models and give the main citations such that further review of the relevant literature can be completed by the interested researcher.

As wireless sensor networks continue to grow and become more common need for security in WSN applications will grow even further. We also expect that the current and future work in privacy and trust will make wireless sensor networks a more attractive option in a variety of new arenas. On the basis of our observation we motivate the need of a security framework to provide countermeasures against attacks in WSNs.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. IEEE Communications Magazine, 40(8):pp.102–114, August 2002.

[2] D. W. Carman, P. S. Krus, and B. J. Matt. Constraints and approaches for distributed sensor network security. Technical Report 00-010, NAI Labs,Network Associates, Inc., Glenwood, MD, 2000.

[3] http://www.zigbee.org/, 2005.

[4] S. Ganeriwal, S. Capkun, C. Han, and M. B. Srivastava. Secure time synchronization service for sensor networks. In WiSe '05: Proceedings of the 4th ACM workshop on Wireless security, pp. 97–106, New York, NY, USA, 2005, ACM Press.

[5] Y. Xiao . Security in Distributed, Grid, and Pervasive Computing, (Eds.) Chapter 17 Auerbach Publications, CRC Press ,2006.

[6] A. D. Wood and J. A. Stankovic. Denial of service in sensor networks. Computer, 35(10):pp . 54–62, 2002.

[7] J. Newsome, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: analysis & defenses. In Proceedings of the third international symposium on Information processing in sensor networks, pp. 259–268. ACM Press, 2004.

[8] J. Deng, R. Han, and S. Mishra. Countermeasures IEEE Computer Magazine against traffic analysis in wireless sensor networks. Technical Report CU-CS-987-04, University of Colorado at Boulder, 2004.

[9] B. Parno, A. Perrig, and V. Gligor. Distributed detection of node replication attacks in sensor networks. In Proceedings of IEEE Symposium on Security and Privacy, May 2005.

[10] X. Wang, W. Gu, K. Schosek, S. Chellappan, and D. Xuan. Sensor network configuration under physical attacks. Technical Report Technical Report (OSU-CISRC-7/ 04-TR45), Dept. of Computer Science and Engineering, The Ohio-State University, July 2004.

[11] T.A.Zia and A.Y. Zomaya. Security issues in wireless sensor networks. In Proceedings of the International Conference on Systems and Networks ICSNC 2006, Nov 2- 4, 2006, Tahiti, French Polynesia.

[12] T. Aura, P. Nikander, and J. Leiwo. Dos-resistant authentication with client puzzles. In Revised Papers from the 8th International Workshop on Security Protocols, pp. 170–177. Springer-Verlag, 2001.

[13] A. Studre and A. Perrig The coremelt attack . In Proceedings of the 14th European Symposium on Research in Computer Security (ESORICS 2009) September 21-23, 2009 Saint-Malo, France.

[14] Y. Hu, A. Perrig, and D. B. Johnson. Packet leashes: A defense against wormhole attacks in wireless networks. In INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies., volume 3, pp. 1976–1986, 2003.

[15] J. Deng, R. Han, and S. Mishra. INSENS: intrusion-tolerant routing in wireless sensor networks. In Technical Report CU-CS-939-02, Department of Computer Science, University of Colorado, 2002.

[16] S. Tanachaiwiwat, P. Dave, R. Bhindwale, and A. Helmy. Poster abstract secure locations: routing on trust and isolating compromised sensors in locationaware sensor networks. In Proceedings of the 1st international conference on Embedded networked sensor systems, pp. 324–325. ACM Press, 2003.

[17] W. Qiu,Y. Zhou,B. Zhu ,Y. zheng,M. Wen and Z. Gong . Key-insulated encryption based key pre-distribution scheme for wsn. Book: Advance in information security and assuurance.volume 557 ,2009, pp. 200-209, Springer Berlin /Heidelbeg,June 18, 2009

[18] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In Proceedings of the 2003 IEEE Symposium on Security and Privacy, pp. 197. IEEE Computer Society, 2003.

[19] S. Zhu, S. Setia, and S. Jajodia. Leap: efficient security mechanisms for largescale distributed sensor networks. In CCS '03: Proceedings of the 10th ACMconference on Computer and communications security, pp. 62–72, New York,NY, USA, 2003. ACM Press

[20] H. Chan and A. Perrig. Pike: Peer intermediaries for key establishment in sensor networks. In IEEE Infocom 2005, 2005.

[21] Q.Huang,J.Cukier,H.Kobayashi, B. Liu, and J. Zhang. Fast authenticated key establishment protocols for self-organizing sensor networks. In Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications, pp. 141–150. ACM Press, 2003.

[22] K. Rasmussen and S. Capkun, . Implications of radio fingerprinting on the security of sensor networks.In Proceeding of the Third International Conference on Security and Privacy for Communication Networks (SecureComm),September 2007.

[23] A. Seshadri, M. Luk, and A. Perrig .SAKE:Software attestation for key establishment in sensor networks,In Proceedings of the 2008 International Conference on Distributed Computing in Sensor Systems (DCOSS), june 2008

[24] R. Di Pietro, L. V. Mancini, Y. W. Law, S. Etalle, and P. Havinga. LKHW: A directed diffusion-based secure multicast scheme for wireless sensor networks. In First International Workshop on Wireless Security and Privacy (WiSPr'03),2003.

[25] L. Lazos and R. Poovendran. Secure broadcast in energy- aware wireless sensor networks. In IEEE International Symposium on Advances in Wireless Communications (ISWC'02), 2002.

[26] L.Lazos and R.Poovendran. Energy-aware secure multicast communication in ad-hoc networks using geographic location information. In Proceedings of IEEE International Conference on Acoustics Speech and Signal Processing ,2003.

[27] T. A. Zia. A security framework for wireless sensor networks, A PhD. thesis submitted to The School of Information Technologies ,The University of Sydney,Australia, February 2008.

[28] www.computer.org/security/cfp.htm.IEEE Security & privacy 2010-03-04.pdf, Vol 8,No 2, March/April 2010 .

[29] H. Chanand and A. Perrig. Round-Effcient broadcast authentication protocols for fixed topology classes. In Proceedings of the IEEE Symposium on Security and Privacy May, 2010 ,Oakland, CA,2010.

[30] Kuldeep and R. Garimella . Distributed key management for wireless sensor networks.Q2SWinet'09,October 28-29 , 2009 , Tenerife , Canary Islands,Spain 2009 .

[31] K. Sharma, M. K. Ghose and Kuldeep.Complete security framework for wireless sensor networks.(IJCSIS),Vol.3,No.1,2009.

[32] K. Sharma, M.K. Ghose, D. Kumar, R. P. Kumar and V. K. Pandey. A comparative study of various security approaches used in wireless sensor networks.(IJAST) ,Vol.17 ,April, 2010.

[33] HBE-Zigbex,Ubiquitous Senser Network,www.hanback.co.kr .