Volume 3, Issue 11, November 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security Threats at Each Layer of Wireless Sensor Networks

Madhumita Panda
Sambalpur University Institute of Information Technology(SUIIT)
Burla, Sambalpur, Orissa, India.

Abstract— Wireless sensor network is a combination of tiny devices called as sensor nodes which have computing, sensing and processing capabilities. Efficient design and implementation of wireless sensor networks have become a hot area of research in recent years due to the vast potential of the sensor networks to enable application that connect the physical world to the virtual world As WSN are deployed in hostile environment usually and can be physically accessible by an adversary; he/she can affect the confidentiality and integrity of the data as well as some other security measures. So security is a main concern for wireless sensor network protocol designers because of the wide security-critical applications of WSNs. This paper deals with the security aspects in the wireless sensor networks giving the probable counter measure for the same.

Keywords - Wireless Sensor Network; Security Requirements; Layer-based Attacks; Countermeasures; Cryptography and Steganography in WSN; Holistic.

I. Introduction

The advances on miniature techniques and wireless communications have made possible the creation and subsequent development of Wireless Sensor Networks (WSN) paradigm. The main purpose of WSN is to serve as an interface to real world, providing physical information such as temperature, light, radiation etc. to a computer system. The major difference between this type of networks and wired networks is their decentralized and specialized nature. In WSN , all its members collaborate towards the common goal of obtaining or deducing certain physical information from their environment. Moreover WSN is capable of self-organization, thus it can be deployed in a certain context without requiring the existence of a supporting infrastructure. As in all the computing environments, it is essential to assure the proper functionality of WSN in order to allow the correct provisioning of services. Such network should comply with certain security requirements, such as confidentiality, integrity, authentication and others derived from application context. However achieving this goal is not an easy task for WSN. The reason is the WSN consists of nodes with very limited resources whereas the attacker may have very powerful attacking (malicious) resources such as laptops with wireless LAN capability, long range wireless communication capability etc. Therefore security in WSN is a major issue. The security techniques of the normal computer networks cannot be implemented in WSN because of limited resources. Considering, for example, the asymmetric cryptographic algorithm (such as RSA with 1024 bits) the memory of a typical sensor node is not sufficient enough to hold even the variables for its implementation. Even if memory is allowed the computation time would be enormous. To worsen the situation the power available with a sensor node is also very small (and the node may entirely consume even in a single computation). So we may conclude that the normal computationally heavy algorithms of security can't be applied on the *weak (*resource limited) *WSN*.

Basically the major challenge for employing any efficient security scheme in wireless sensor networks is created by the size of sensors, consequently the processing power, memory and type of tasks expected from the sensors. We discuss these issues and challenges in this paper.

The paper is organized as follows. Section 2 describes the operation of Wireless Sensor Networks. Section 3 describes the security classes. Section 4 explores various types of threats and attacks against wireless sensor network with probable countermeasures. To address the critical security issues in wireless sensor networks Section 5 talks about cryptography, steganography. Section 6 reviews the related works and proposed schemes concerning security in WSN and also introduces the view of holistic security in WSN. Finally Section 7 concludes the paper delineating the research challenges and future trends toward the research in wireless sensor network security.

II. Operation

A WSN is a large network of resource-constrained sensor nodes with multiple preset functions, such as sensing and processing, to fulfil different application objectives. The major elements of WSN are the sensor nodes and the base stations. In fact, they can be abstracted as the "sensing cells" and the "brain" of the network, respectively. Usually, sensor nodes are deployed in a designated area by an authority and then automatically form a network through wireless communications. Sensor nodes are static most of the time, whereas mobile nodes can be deployed according to application requirements. One or several, static or mobile base stations (BSs) are deployed together with the network. Sensor nodes keep monitoring the network area after being deployed. After an event of interest occurs, one of the surrounding sensor nodes can detect it, generate a report, and transmit the report to a BS through multihop wireless links.

Collaboration can be carried out if multiple surrounding nodes detect the same event. In this case, one of them generates a final report after collaborating with other nodes. The BS can process the report and then forward it through either high quality wireless or wired links to the external world for further processing .The WSN authority can send commands or queries to a BS, which spreads those commands or queries into the network. Hence, a BS acts as a gateway between the WSN and the external world. An example is shown in Figure 1.

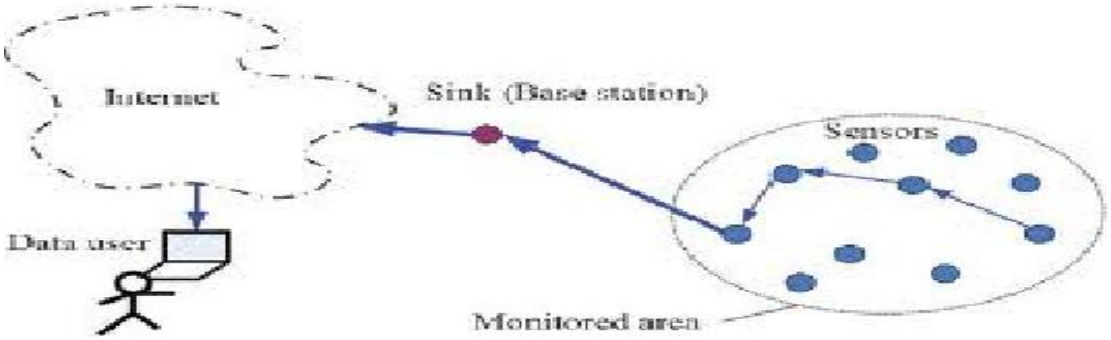

Fig. 1: Wireless sensor network

Most of the research on this topic is revolved around security solutions using a layered approach. The layered approach is shown in Figure. 2. In layered approach the protocol stacks consists of the physical layer, data link layer, network layer, transport layer and application layer. These five layers and the three planes, i.e., power management plane, mobility management plane and the task management plane jointly forms the wireless layered architecture.

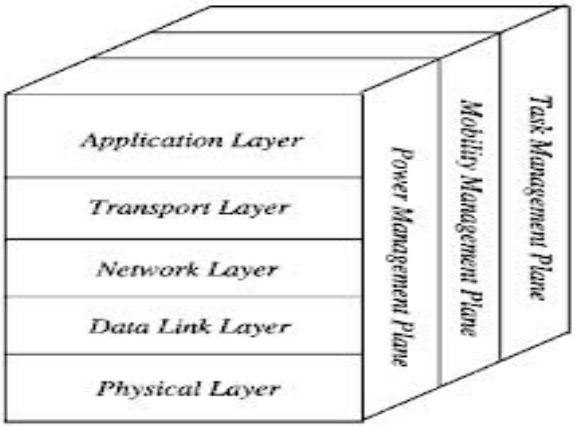

Fig. 2: Generic Protocol Stack for Sensor Networks

III. Security Classes

Attacks on wireless network can be broadly classified as interception, modification and fabrication.

- Interception is an attack on confidentiality. The sensor network can be compromised by an adversary to gain unauthorised access to sensor nodes or data within it.
- Modification is an attack on integrity. Modification means an unauthorised party not only accesses the data but tampers it, for example by modifying the data packets being transmitted.
- Fabrication is an attack on authentication. In fabrication, an adversary injects false data and compromises the trustworthiness of the information relayed.

IV. Network Security Threats

This section discusses about the WSN layer wise attack.

Sensor network security in Physical Layer

The physical layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation and data encryption.[1].

The most common attacks on physical layer are as follows:-

Jamming

Jamming is a type of attack which interferes with the radio frequencies that a network's nodes are using [2].A jamming source may either be powerful enough to disrupt the entire network or less powerful and only able to disrupt a smaller portion of the network. Even with lesser-powered jamming sources, such as a small compromised subset of the network's sensor nodes, an adversary has the potential to disrupt the entire network provided the jamming sources are randomly distributed in the network. Typical defenses against jamming involve variations of spread-spectrum communication such as frequency hopping and code spreading. Frequency-hopping spread spectrum (FHSS) is a method of transmitting signals by rapidly switching a carrier among many frequency channels using pseudorandom sequence known to both transmitter and receiver. Without being able to follow the frequency selection sequence, an attacker is unable to jam the

frequency being used at a given moment in time. However, as the range of possible frequencies is limited, an attacker may instead jam a wide section of the frequency band. Code spreading is another technique used to defend against jamming attacks and is common in mobile networks. However, this technique requires greater design complexity and energy, thus restricting its use in WSNs. In general, to maintain low cost and low power requirements, sensor device are limited to single-frequency use and are therefore highly susceptible to jamming attacks.

Tampering

Sometimes the nodes are physically tampered by an adversary. Such condition is called tampering [3]. A tampering attacker may damage, replace and electronically interrogate the nodes to acquire information [4].

One defence to this attack involves tamper-proofing the node's physical package. Self Destruction (tamper-proofing packages)-whenever somebody accesses the sensor nodes physically the nodes vaporize their memory contents and this prevents any leakage of information. Second-Fault Tolerant Protocols-the protocols designed for a WSN should be resilient to this type of attacks.

Radio interference

In which the adversary either produces large amounts of interference intermittently or persistently. To handle this issue, use of symmetric key algorithms in which the disclosure of the keys is delayed by some time interval.

Sensor network security issues at the Data Link Layer

The objective of this Layer is to insure interoperability amongst communication between nodes to nodes. The Data Link layer is responsible for the multiplexing of data streams, data frame detection, medium access, and error control [1]. The data link layer is vulnerable due to the reason that the data is transmitted in an open insecure medium. Hence it is susceptible to the attacks on the authenticity, integrity and confidentiality of the data being routed[5].

The main attacks at the data link layer are as follows:-

Collision

A collision occurs when two nodes attempt to transmit on the same frequency simultaneously. When packets collide, a change will occur in the data portion, causing a checksum mismatch at the receiving end. The packet will then be discarded as invalid .A typical defence against collisions is to use error- correcting codes.

Jamming

Jamming can occur when the data get jammed with radio signals from other transmissions[3].

Continuous Channel Access (Exhaustion)

A malicious node disrupts the Media Access Control protocol, by continuously requesting or transmitting over the channel. This eventually leads a starvation for other nodes in the network with respect to channel access. One of the countermeasures to such an attack is Rate Limiting to the MAC admission control such that the network can ignore excessive requests, thus preventing the energy drain caused by repeated transmissions. A second technique is to use time division multiplexing where each node is allotted a time slot in which it can transmit.

Unfairness

Repeated application of these exhaustion or collision based MAC Layer attacks or an abusive use of cooperative MAC Layer priority mechanisms can lead into unfairness. This kind of attack is a partial DOS attack, but results in marginal performance degradation. One major defensive measure against such attacks is the usage of small frames, so that any individual node seizes the channel for a smaller duration only.

Sensor network security issues at Network layer

The objective of Network layer is to find the best path for efficient routing mechanism. This layer is responsible for routing the data from node to node, node to sink ,node to base station, node to cluster head and vice versa.

Vulnerabilities at network layer are as follows:-

Selective Forwarding

Normally the sensor networks are multi-hop systems. So, the sensors pass information from one end to the base station by routing them through intermediate nodes. Sometimes a malicious node may be present within the network path. In a flooding based protocol, the attacker (malicious node) listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. [6] Then the target may choose the route which contains the malicious node. Malicious or attacking nodes can however refuse to route certain messages and drop them. The result is loss of huge amount of data, during the multi-hop information exchange process. In another case it may happen that the malicious node drops all the packets it receives, hence no information is forwarded. This creates a *black hole*. Such attacks are effective when the attacker is explicitly included in the data path of sensor network.

One defence against selective forwarding attacks is using multiple paths to send data [7].A second defence is to detect the malicious node or assume it has failed and seek an alternative route.

Sinkhole Attack

Attracting traffic to a specific node in called sinkhole attack. In this attack, the adversary's goal is to attract nearly all the traffic from a particular area through a compromised node. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes. [8]. Since now most of the data is being routed through the malicious node, the attacker/malicious node can play anything with the sensor data. [9] Many other attacks such as wormhole, selective forwarding or eavesdropping can be initiated through this sinkhole attack.

Geo-routing protocols are known as one of the routing protocol classes that are resistant to sinkhole attacks, because that topology is constructed using only localized information, and the traffic is naturally routed through the physical location of the sink node, which makes it difficult to lure it elsewhere to create a sinkhole.

Sybil Attack

The Sybil attack is a case where one node presents more than one identity to the network [2,7,10].This may mislead other nodes as shown in Figure 3 below, and hence routes believed to be disjoint with respect to node can have the same adversary node. A countermeasure to Sybil Attack is by using a unique shared symmetric key for each node with the base station.

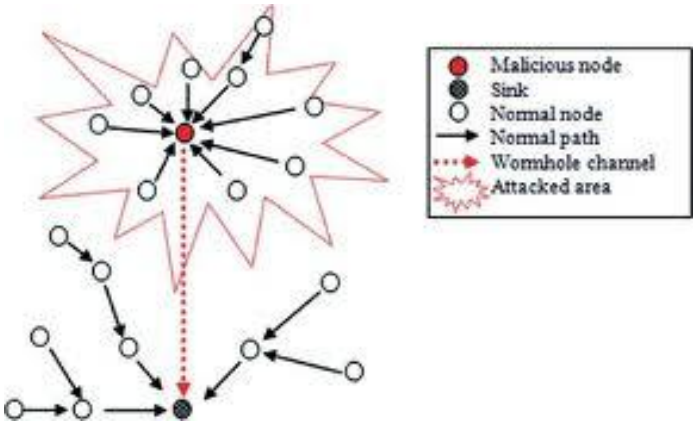

Fig.3.Sybil Attack

Wormholes Attacks

A wormhole is a low-latency link between two portions of the network over which an attacker replays net-work messages [7]. This link may be established either by a single node forwarding messages between two adjacent but otherwise non-neighboring nodes or by a pair of nodes in different parts of the network communicating with each other. The latter case is closely related to the sinkhole attack, as an attacking node near the base station can provide a one-hop link to that base station via the other attacking node in a distant part of the network. Huet al. presented a novel and general mechanism called packet leashes for detecting and defending against wormhole attacks [11]. Two types of leashes were introduced: geographic leashes and temporal leashes. The proposed mechanisms can also be used in WSNs.

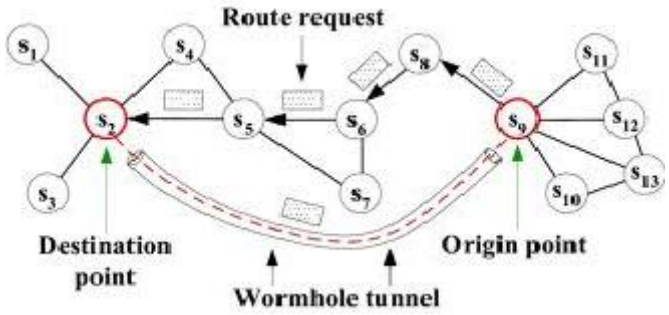

Fig.4. Wormhole Attack

Hello Flood Attacks

Many protocols which use HELLO packets make the naive assumption that receiving such a packet means the sender is within radio range and is therefore a neighbor. An attacker may use a high-powered transmitter to trick a large area of nodes into believing they are neighbors of that transmitting node [7]. If the attacker falsely broad casts a superior route to the base station, all of these nodes will attempt transmission to the attacking node, despite many being out of radio range in reality.

Acknowledgment Spoofing

Routing algorithms used in sensor networks sometimes require Acknowledgments to be used. An attacking node can spoof the Acknowledgments of overheard packets destined for neighboring nodes in order to provide false information to those neighboring nodes [7]. An example of such false information is claiming that a node is alive when in fact it is dead.

Sensor network security issues at Transport layer

The transport layer is responsible for managing end-to-end connections [1].Sometimes an attacker might be strong enough to reach up to the transport layer, due to attack being undetected at the lower layers[3].
Two possible attacks in this layer, flooding and desynchronization are discussed in this subsection.

Flooding

An attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit**.** It produces severe resource constraints for legitimate nodes. One proposed solution to this problem is to require that each connecting client demonstrate its commitment to the connection by solving a puzzle. As a defense against this type of attack, a limit can be put on the number of connections from a particular node.

De-synchronization Attacks

In this attack, the adversary repeatedly forges messages to one or both end points which request transmission of missed frames. Hence these messages are again transmitted and if the adversary maintains a proper timing it can prevent the endpoints from exchanging any useful information .This will cause a considerable drainage of energy of legitimate nodes in the network in an end less synchronization-recovery protocol. A possible solution to this type of attack is to require authentication of all the packets including control fields communication between hosts. Header or full packet authentication can defeat such an attack.

Sensor network security issues at Application layer

The objective of Application Layer is to present final output by ensuring smooth information flow to lower layers. This layer is responsible for data collection, management and processing of the data through the application software for getting reliable results. Main attack at application layer is attacks on reliability.

Attacks on reliability

If an adversary changes the data in one path then it puts a question mark on the reliability of the data. In this attack attacker needs to identify the path of communication and put adversary in that path to change the data. An adversary can generate false data or query by joining the network. When a node responds to these wrong data or query, leads them to suffer from the energy drain attack. Usually to ensure reliability acknowledgement is expected for each successful data delivery [12].

V. Cryptography in WSN

WSN are used in many critical applications like military, habitat monitoring etc. Minimum level of security like integrity and authentication is required for certain applications, due to their sensitive nature of data. This type of security can be provided by using any cryptography scheme in WSN. Cryptography aims at making data not understandable to any unauthorized party which has the goal of data interpretation. But, it is difficult to choose the appropriate scheme because of resource/computation constrained nature of WSN. PKC (Public key cryptography) is not suitable for WSN because of its resource demanding nature [13,14]. SKC (symmetric key cryptography) is more efficient and suitable for WSN. But, it has the inherent problem of sharing the secret keys and also, the hostile nature of WSN makes it vulnerable to various attacks [13, 14].In order to encrypt or decrypt data, first of all keys should be distributed among nodes. This is the goal of key management system. It is also responsible for revoking and refreshing keys in order to gain better security. For any key establishment technique to be efficient, it should support several requirements like in-network processing and facilitating self-organization of data. However, Key establishment technique should minimally support authenticity, confidentiality, integrity, flexibility and scalability [15].

5.1 Steganography

While cryptography aims at hiding the content of a message, steganography [16], [17] aims at hiding the existence of the message. Steganography is the art of covert communication by embedding a message into the multimedia data (image, sound, video, etc.) [18]. The main objective of steganography is to modify the carrier in a way that is not perceptible and hence, it looks just like ordinary. It hides the existence of the covert channel, and furthermore, in the case that we want to send a secret data without sender information or when we want todistribute secret data publicly, it is very useful. However, securing wireless sensor networks is not directly related to steganography and processing multimedia data (like audio, video) with the inadequate resources [19] of the sensors is difficult and an open research issue.

VI. Proposed Security Schemes and Related Work

In the recent years, wireless sensor network security has been able to attract the attentions of a number of researchers around the world. In this section we review and map various security schemes proposed or implemented so far for wireless sensor networks.

6.1. Security Schemes for Wireless Sensor Networks

Newsome et. al. [20] proposes some defense mechanisms against sybil attack in sensor networks. SNEP & μTESLA [21] are two secure building blocks for providing data confidentiality, data freshness and broadcast authentication.

[22] gives an analysis of secure routing in wireless sensor networks. [23] studies how to design secure distributed sensor networks with multiple supply voltages to reduce the energy consumption on computation and therefore to extend the network's life time. [24] aims at increasing energy efficiency for key management in wireless sensor networks and uses Younis et. al. [25] network model for its application. JAM [26] presents a mapping protocol which detects a jammed region in the sensor network and helps to avoid the faulty region to continue routing within the network, thus handles DoS attacks caused by jamming. In [27] the authors show that wormholes those are so far considered harmful for WSN could effectively be used as a reactive defense mechanism for preventing jamming DoS attacks. Ye et. al. [28] presents a statistical en-route filtering (SEF) mechanism to detect injected false data in sensor network and focus mainly on how to filter false data using collective secret and thus preventing any single compromised node from breaking the entire system. .TinySec [29] proposes a link layer security mechanism for sensor networks which uses an efficient symmetric key encryption protocol. Kulkarni et al. [30]analyzes the problem of assigning initial secrets to users in ad-hoc sensor networks to ensure authentication and privacy during their communication and points out possible ways of sharing the secrets. Currently much of work is going on providing layered security for example in Holistic Security Approach [31].

6.2Holistic Security in Wireless Sensor Networks

A holistic approach [32] improves the performance of wireless sensor networks with respect to security, longevity and connectivity under changing environmental conditions. The holistic approach of security concerns about involving all the layers for ensuring overall security in a network. For such a network, a single security solution for a single layer might not be an efficient solution rather employing a holistic approach could be the best option.

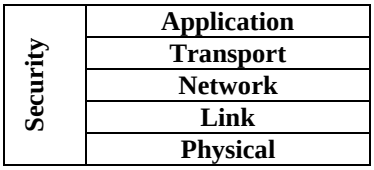

Fig 5: Holistic view of Security in wireless sensor networks

In holistic approach security is to be ensured for all the layers of the protocol stack, the cost for ensuring security should not exceed the assessed security risk at a specific time, the security measures must be able to exhibit a graceful degradation if there is no physical security ensured for the sensors and if some of the sensors in the network are compromised, out of order or captured by the enemy and the security measure should be developed to work in a decentralized fashion. If security is not considered for all of the security layers, for example; if a sensor is somehow captured or jammed in the physical layer, the security for the overall network breaks despite the fact that, there are some efficient security mechanisms working in other layers. By building security layers as in the holistic approach, we can improve the security for the whole network.

VII. Conclusion

Providing security in a wireless sensor network is a challenging task. In this paper, we have discussed various security threats expected at different layer of WSN protocol stack. Possible solution against each threat is also outlined. Detection and countermeasures of some threats in WSN is not at all easy. Key distribution among sensor nodes is also a challenging task. In present time, most of the security schemes are based on specific network models and complete security model for all layers is not at all present although, in future, the security
scheme might become well established for individual layer.

References

[1] .I.F.Akyildiz et al.,"A Survey on Sensor Networks",*IEEE Commun.Mag.*,vol.40,no.8,Aug.2002,pp.102-114.

[2]. .E.Shi and A.Perrig,"Designing Secure Sensor Networks, "Wireless Commun. Mag.,vol.11,no.6,Dec.2004 pp.38-43.

[3]. Anitha S.Sastry,Shazia Sulthana and Dr.S Vagdevi."Security Threats in Wireless Sensor Networks in Each Layer",Int.J.Advanced Networking and Applications,Volume:04 Issue 04 Pages:1657-1661(2013).

[4]. Shahnaz Saleem,Sana Ullah,Hyeong Seon Yoo"on the Security Issues in Wireless Body Area Networks"International Journal of Digital Content Technology and its Applications Volume 3,number3,September 2009.

[5]. Asif Habib "Sensor Network Security Issues at Network Layer",2nd International Conference on Advaificances in Space Technologies,Pp.58-63 National Engineering and Scientific Commission Islamabad,Pakistan.

[6]. Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong,"Security in Wireless Sensor Networks: Issues and Challenges",International Conference on Advaificances in Space Technologies.

[7]. C.Karlof and D.Wagner,"Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures" ,Proc. First IEEE Int'l Wksp. Sensor Network Protocols and Applications ,May 2003,pp.113-27.

[8]. Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", AdHoc Networks (elsevier), Page: 299-302, year 2003.

[9]. Haowen Chan,and Adrian Perrig,"Security and Privacy in Sensor Networks",Carnegie Mellon University pp.99-101.

[10]. J.Newsome et al., "The Sybil Attack in Sensor Networks: Analysis and Defenses",IPSN'04:Proc.IEEE Int'l. Conf. Info. Processing in Sensor Networks,Apr.2004.

[11]. Y.C.Hu,A.Perrig,and D.B.Johnson,"Packet Leashes:A defense Against Wormhole Attacks in Wireless Networks",Proc.IEEE INFOCOM 2003,Apr.2003.

[12]. Prabhudutta mohanty,Sangram Panigrahi,Nityananda Sarma and Siddhartha Sankar Satpathy""Security issues in wireless sensor network data gathering protocols:a survey",journal of Theoritical and Applied Information Technology.

[13]. Ali Tufail, Ki-Hyung Kim, "A Backbone Assisted Hybrid Key Management Scheme for WSN", IEEE 978-0-9564263-8/3 (2011).

[14]. Huan-Chung Lin and Yuh-Min Tseng, "A Scalable ID-Based Pair wise Key Establishment Protocol for Wireless Sensor Networks" , Journal of Computers (2008).

[15]. Yang Xiao, Venkata Krishna Rayi , Bo Sun , Xiaojiang Du , Fei Hu ,Michael Galloway, "A survey of key management schemes in wireless sensor networks", Computer Communications 30 (2007) 2314–2341.

[16]. Kurak, C and McHugh, J, "A Cautionary Note on Image Downgrading in Computer Security Applications", Proceedings of the 8th Computer Security Applications Conference, San Antonio, December, 1992, pp. 153-159.

[17]. Mokowitz, I. S., Longdon, G. E., and Chang, L., "A New Paradigm Hidden in Steganography", Proc. of the 2000 workshop on New security paradigms, Ballycotton, County Cork, Ireland, 2001, pp. 41 – 50.

[18]. Kim, C. H., O, S. C., Lee, S., Yang, W. I., and Lee, H-W., "Steganalysis on BPCS Steganography", Pacific Rim Workshop on Digital Steganography (STEG'03), July 3-4, Japan , 2003.

[19]. Younis, M., Akkaya, K., Eltoweissy, M., and Wadaa, A., "On handling QoS traffic in wireless sensor networks", Proc. of the 37th Annual Hawaii International Conference on System Sciences, 2004, 5-8 January, 2004, pp. 292 – 301.

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

[21]. Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D., "SPINS: Security Protocols for Sensor Networks", Wireless Networks, vol. 8, no. 5, 2002, pp. 521-534.

[22]. Karlof, C. and Wagner, D., "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003, pp. 293-315.

[23]. Yuan, L. and Qu, G., "Design space exploration for energy-efficient secure sensor network", Proc. The IEEE International Conference on Application-Specific Systems, Architectures and Processors, 2002, 17-19 July 2002, pp. 88 – 97.

[24]. Jolly, G., Kuscu, M.C., Kokate, P., and Younis, M., "A Low-Energy Key Management Protocol for Wireless Sensor Networks", Proc. Eighth IEEE International Symposium on Computers and Communication, 2003. (ISCC 2003). vol.1, pp. 335 - 340

[25]. Younis, M., Youssef, M., and Arisha, K., "Energy-aware routing in cluster-based sensor networks" Proc. 10th IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunications Systems, 1-16 Oct. 2002 pp. 129 – 136.

[26]. Wood, A.D., Stankovic, J.A., and Son, S.H., "JAM: A Jammed-Area Mapping Service for Sensor Networks", 24th IEEE Real-Time Systems Symposium, RTSS 2003, pp. 286-297.

[27]. Cagalj, M., Capkun, S., and Hubaux, J-P., "Wormhole-based Anti-Jamming Techniques in Sensor Networks" from http://lcawww.epfl.ch/Publications/Cagalj/CagaljCH05-worm.pdf. .

[28]. Ye, F., Luo, H., Lu, S, and Zhang, L, "Statistical en-route filtering of injected false data in sensor networks", IEEE Journal on Selected Areas in Communications, Volume 23, Issue 4, April 2005, pp. 839 – 850.

[29]. Karlof, C., Sastry, N., and Wagner, D., "TinySec: a link layer security architecture for wireless sensor networks", Proc. of the 2nd international conference on Embedded networked sensor systems, Baltimore, MD,USA, 2004, pp. 162 – 175.

[30]. Kulkarni, S. S., Gouda, M. G., and Arora, A., "Secret instantiation in adhoc networks," Special Issue of Elsevier Journal of Computer Communications on Dependable Wireless Sensor Networks, May 2005, pp. 1–15.

[31]. Al-Sakib Khan Pathan et. al. "Security in Wireless Sensor Networks: Issues and Challenges" in Feb. 20-22, 2006, ICACT2006, ISBN 89-5519-129-4 pp(1043-104

[32]. Avancha, S, "A Holistic Approach to Secure Sensor Networks", PhD Dissertition, University of Maryland, 2005.

