Security Overview of Wireless Sensor Network

Hero Modares[1], Amirhossein Moravejosharieh[2], Rosli Salleh[3], Jaime Lloret[4]

[1,3]Department of Computer system and technology, University of Malaya, Kuala Lumpur, Malaysia
[2]Department of Computer, Science and Engineering, University of Canterbury, Christchurch, New Zealand
[4]Department of Communications, Polytechnic University of Valencia, Camino de Vera s/n,Valencia, Spain
Hero.Modares@gmail.com

Abstract: There are several types of security threats that can give rise to vulnerability issues and performance degradation for the Wireless Sensor Network (WSN). The existing protocols that incorporate security features for authentication, key management, and secure routing, have not able to protect the WSN, effectively but a new Intrusion Detection System (IDS) can overcome these problems. The IDS collects data for analysis in order to identify any abnormal behaviour at the sensor nodes, which if present, could indicate an attack on the network. Many different intrusion detection systems for wireless sensor networks have been proposed in the past years. This paper focuses on the security requirements, layering-based attacks, and intrusion detection in WSN.

[Hero Modares, Amirhossein Moravejosharieh, Rosli Salleh, Jaime Lloret. **Security Overview of Wireless Sensor Network.** *Life Sci J* 2013;10(2):1627-1632]. (ISSN:1097-8135). http://www.lifesciencesite.com. 225

Keywords: Wireless Sensor Network (WSN), Security Requirement, Layering-based attacks, Intrusion Detection System (IDS)

1. Introduction

The distributed wireless technology in sensor networks has been applied various types of systems and applications. RF communication is used to link together the huge number of wireless sensors in a wireless sensor network (WSN). These nodes are responsible for gathering and distribution of information in the network. The network and nodes can be affected by different types of attacks. If an affected node is still running and exchanging data across the network, it could lead to loss of its power supply and could, in the worst case scenario, eventually become a dead node (Anisi, Abdullah, & Razak, 2012; Babaie, Khadem-zadeh, & Badie, 2012; Bidgoli, Pajouhesh, & Ahmadi, 2011; Khan, Loo, & Din, 2010; Krontiris, Benenson, Giannetsos, Freiling, & Dimitriou, 2009; Rajani Muraleedharan & Osadciw, 2006; P. Sharma, Sharma, & Singh, 2012). In addition, because of limited resources, some WSN applications are not able to take advantage of certain network security features. The Quality of Service (QoS) could be affected because of the small node size. In the WSN, battery power supply is very limited and this restricts the amount of memory that could be used for optimum performance (Kavitha & Haritha, 2011; Ranjani Muraleedharan & Osadciw, 2003; Noack & Spitz, 2009; Sahadevaiah & PVGD, 2011; K. Sharma & Ghose, 2010). This paper focuses on the security requirements, layering-based attacks, and intrusion detection in the WSN. In section 2 will go through the security requirement in WSN, section 3 will focus on layering-based attacks, in section 4 we will explain the IDS in WSN, in section 5 we will describe the cryptography in WSN, finally section 6 is the conclusion.

2. Security Requirements

A sensor network can be considered to be a special type of network, which likewise, has specific security requirements, these requirements are mainly related to the data confidentiality; data integrity; data freshness; network availability; and data authenticity (Carman, Kruus, & Matt, 2000; Modares, 2009; Modares, Salleh, & Moravejosharieh, 2011; Mohanty, Panigrahi, Sarma, & Satapathy, 2010; Perrig, Szewczyk, Tygar, Wen, & Culler, 2002; Walters, Liang, Shi, & Chaudhary, 2007; Yoneki & Bacon, 2005):

2.1. Data Confidentiality

Data confidentiality is the most critical issue in network security. In sensor networks, data confidentiality is related to the following:

- The readings from the sensor in any network should not be leaked to neighbouring sensors. The information from these readings could be very sensitive, especially, information for military use.
- A secure channel for data transmission, as data in many applications is highly sensitive, for example, the distribution of keys across the network.
- The public information of the sensor such as sensor identity and public keys, should be encrypted to ensure protection against traffic analysis type-attacks.

Data encryption has become the standard method

for protecting the sensitive data, thus, protecting data confidentiality, is general.

2.2. Data Integrity

Data integrity is concerned with ensuring that information is not modified or altered during communication. Effective security measures must be implemented to prevent a malicious mode or an attacker from changing the data or information that can cause the network to go disarray.

2.3. Data Freshness

It is important that only the latest or most recent messages are delivered. In other words, the data must remain "fresh" at all times. This is particularly important when shared-key strategies are implemented in the network, because shared-keys are altered, constantly for security. Malicious attackers can launch a replay attack because these keys take time to propagate throughout the network. The network can also be disrupted if the sensors do not know when to change the keys. This problem can be overcome by including a nonce or time-related counter in the data packet to guarantee freshness.

2.4. Availability of the Network

Network availability is concerned about the stable operation and availability of the network as a whole. Additional costs are incurred to modify the traditional encryption algorithms for a WSN. Thus, some approaches avoid these costs by modifying and recycling the codes as much as possible, while others use different methods of communication in a WSN. Another approach enforces strict limitation on data access, and proposes some inappropriate schemes to simplify the algorithm. Most of these approaches, however, weaken the sensors and reduces network availability because of the following reasons:

- Power supply is required for additional computing, thus, if it is not available, then, there can be no access to the data.
- Power supply is also required for additional communication. If communication traffic increases, then the chances of conflicts also increase.

If a centralised scheme is implemented, failure event at a single point might adversely affect the availability of the network.

2.5. Authentication

Data authentication is about ensuring that data received by a node for any decision-making process must come from the correct source. It is known that attackers will also insert additional packets into the packet stream besides modifying the data packets, to cause disruptions. During the construction of the sensor network, the authentication process is important for executing administrative tasks, for example, network programming, controlling the sensor node duty cycle, etc. Authentication is also very important to many sensor network applications. Data verification assures the receivers that the data they receive is sent from the correct sender. A pure symmetric mechanism is used for data authentication in a two-party communication. Using this method, the sender and receiver share the same secret key to generate the MAC (Message Authentication Code) for all the transmitted data packets. Perrig et al. (2002) proposed the use of a key-chain distribution system for their µTESLA secure broadcast protocol. It is aimed at achieving asymmetric cryptography by delaying the disclosure of the symmetric keys. The sender broadcasts a message using a secret key, which will be disclosed only after a certain time. Until the key is disclosed, the receiver will buffer all the packets. Once the secret key is disclosed, the packets will be authenticated provided that it had been received before the disclosure of the secret key. However, the disadvantage is that some preliminary information must be unicasted to every sensor before the authentication process can begin.

Liu and Ning (Liu & Ning, 2003, 2004) proposed an enhancement to the µTESLA system. Their system involved broadcasting, rather than unicasting, the key chain commitments. Several methods were proposed, ranging from those involving simple and pre-determined key chains to those involving the multi-level key chain. In order for a scalable key to be achievable, pre-determination and broadcasting are applied to the multi-level key chain scheme. This is primarily aimed at mitigating the denial of service attacks, and jamming.

3. Layering-based attacks

3.1. Physical Layer

Jamming is one of the well-known methods of physically attacking a wireless network. It will cause interference to the node's radio frequency in the network. The attacker sequentially transmits, and refuses the underlying MAC protocol of the wireless network. This can cause serious interruptions to the network traffic, especially, if only one frequency is used in the network. It can also cause the nodes to use excessive amount of energy due to the insertion of irrelevant packets into those nodes (Kim, Kim, & Choi, 2009).

Xu, Trappe, Zhang and Wood (2005) identified four different types of jamming attacks that can seriously disrupt or stop the wireless network operations. They wanted to assess the effect of jamming on the nodes during the sending and the receiving processes. However, they lacked the appropriate measuring system (for carrier

sensing time and signal strength) to evaluate the effect of the jamming attacks. Also, even with clear difference between the two conditions, using packet deliveries would not show the cause of poor link (from node mobility or jamming) in the network (Xu, Trappe, Zhang, & Wood, 2005).

Another type of physical attack is tampering, which causes physical damages to the nodes (Jeon, 2006). Table 1, below, lists the physical layer threats and the countermeasures against those threats (Kalita & Kar, 2009).

Table 1: Physical Layer Threats

Threat	***Countermeasure***
Interference	Channel hopping and Blacklisting
Jamming	Channel hopping and Blacklisting
Sybil	Physical protection of the devices
Tampering	Protection and changing of keys

3.2. Data Link Layer

Aside from the physical layer, the link layer is also open to malicious attacks. Attackers can premeditatedly ignore or violate the communication protocols and send messages frequently in an attempt to cause collisions. Packets affected by the collision will have to be re-transmitted. In this attack, the adversary can force an excessive amount of retransmission on a node and cause its power supply source to be totally exhausted (Walters, et al., 2007). Table 2 below shows the data link layer threats and the countermeasures against them (Kalita & Kar, 2009).

Table 2: Data-Link Layer Threats

Threat	***Countermeasure***
Collision	CRC and Time diversity
Exhaustion	Protection of network ID and other information that is required to joining device
Spoofing	Use different path for re-sending the message
Sybil	Regularly changing of keys
De-synchronization	Using different neighbours for time synchronization
Traffic analysis	Sending of dummy packet in quiet hours: and regular monitoring WSN network
Eavesdropping	Key protects DLPDU from eavesdropper

3.3. Network Layer

The sensor node benefits from multi-hopping by simply refusing to route messages at the network layer. This can happen frequently or irregularly, and will result in neighbouring node that marks the route, not being able to exchange messages with other nodes in the network (Walters, et al., 2007; Wood & Stankovic, 2002).

Attacks in the form of forced entry or access without authorisation into the network layer, can be divided into two categories: passive, and active. In a passive attack, an attacker trespasses without interrupting the running of the network. The attacker is only looking for information, and eavesdropping on the network traffic without modifying any data. It is quite difficult to detect passive attacks because they do not change any functions of the node or the network.

Active attacks are, however, totally the opposite of passive attacks. These attacks interfere with the network by modifying the messages that contain data packets and routing control packets. An attacker uses the routing packets to cause havoc on the network and force the creation of useless routing table to be created at the source.

The attacker can also cause the communication to be broken by attacking data packets, even though it assists other nodes by creating a legal route between both the sender and the receiver. Some examples of active attacks are Wormhole attacks (Y-C Hu, Adrian Perrig, & David B Johnson, 2003), Blackhole attacks (Deng, Li, & Agrawal, 2002), Byzantine attacks (Awerbuch, Holmer, Nita-Rotaru, & Rubens, 2002), DDoS attacks (Enck, Traynor, McDaniel, & La Porta, 2005) and routing attacks (Yih-Chun Hu, Adrian Perrig, & David B Johnson, 2003; Peter, Langendorfer, & Piotrowski, 2008). Active attacks can also be categorised based on whether they target the data plane or the control plane, for example, key distribution or routing protocols.

Encryption schemes and hash functions are commonly used to maintain data integrity and proper authentication. The centralised key management approach is also used in tandem with the encryption methods. The Certification of Authority is applied in the public keys as a way of effecting node communication security (Jeon, 2006). Table 3, below, shows the network layer threats and the countermeasures against those threats (Kalita & Kar, 2009):

Table 3: Network Layer Threats

Threat	**Countermeasure**
Eavesdropping	Session keys protect NPDU from eavesdropper.
DoS	Protection of network-specific data link network ID etc. Physical protection and inspection of network.
Selective forwarding	Regular network monitoring using source routing.
Sybil	Resetting of device and changing of session keys.
Traffic Analysis	Sending of dummy packet in quiet hours: and regular monitoring of WSN network.
Wormhole	Physical monitoring of field devices, and regular monitoring of the network using Source Routing. Monitoring system may use packet leach

3.4. Transport Layer

The transport layer is also vulnerable to attacks, particularly, flooding attacks. It can be as

simple as sending large number of connection requests to a vulnerable node. In this attack, sender is assigned to manage the request for a connection, which would lead to the depletion and exhaustion of the node's resources. Eventually, the node will be rendered useless (Walters, et al., 2007).

4. Intrusion Detection in Wireless Sensor Networks

In a typical wireless sensor network, cryptography is often used as a method to secure the network against entries from external unauthorised nodes. However, cryptography is unable to prevent attacks from nodes that possess several of the keys. Brutch and Ko (2003) divided the intrusion detection system (IDS) into two categories: host-based system and network-based system. They further categorise them as signature-based system, anomaly-based system, and specification-based system. The host-based IDS operates through the OS audit trails, the system calls audit trail, logs, etc, while, the network-based IDS operates on the packets that are captured in the network (Brutch & Ko, 2003).

The role of signature-based IDS is to monitor the network for the presence of certain signatures that could indicate intrusion. The anomaly-based IDS define, a standard behaviour pattern and any behaviour that deviates from the standard pattern, is an indication of an intrusion into the system. The specification-based IDS follows a set of constraints that are specific to the correct operation of the program or network (Brutch & Ko, 2003).

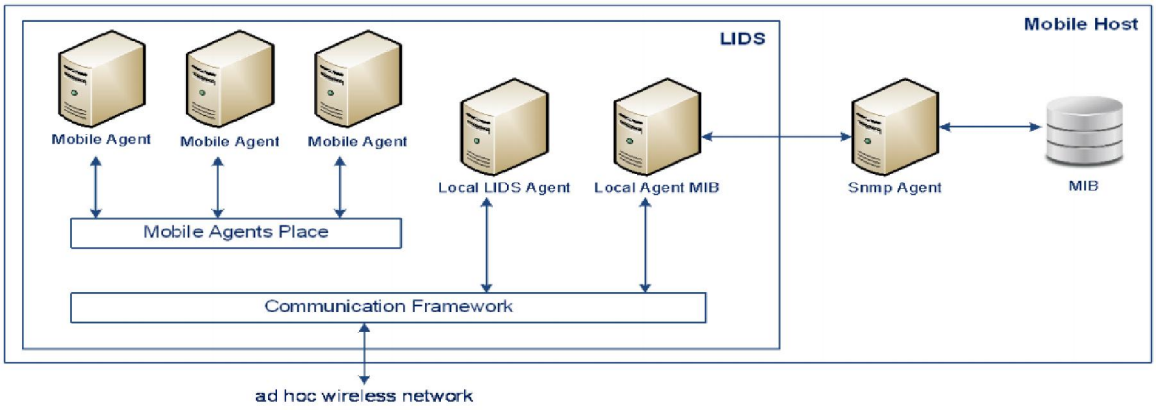

Figure 1: The LIDS architectur

Brutch and Ko have also described various types of attacks on the wireless sensor networks, and introduced three architectures to detect intrusions in the network. In first architecture, known as the stand-alone architecture, every node in the network functions as an independent intrusion detection system. These nodes are responsible for detecting any possible attacks, which are directed them. Each node acts on its own and does not cooperate while other nodes, in any way(Brutch & Ko, 2003).On the other hand, the second architecture follows the distributed and cooperative approach. Each node contains an intrusion detector and is responsible for detecting intrusion on itself (local attacks), but all the nodes cooperate with each other to share information and to provide support against global intrusion attempts. The third architecture which is the hierarchical architecture, is more suitable for protecting multi-layered wireless sensor network. Brutch and Ko described the multi-layered network as one network but divided into different clusters, and the routing responsibility falls on the cluster head. This multi-layered network can be mainly used for event correlation. Albers et al. Suggested that the intrusion detection architecture on each node should be based on the local intrusion detection system (LIDS). (Albers et al., 2002).

In order for the nodes "vision" or design to be extended across the network, Albers suggested that the LIDS within the network should work with one another. There are two types of information being exchanged within the network: (1) security data – a method to simplify exchange of information with the hosts from other networks; and (2) intrusion alerts – a method to inform about locally detected intrusions to other LIDS (Albers, et al., 2002). Figure 1 shows a pictorial representation of the LIDS architecture.

By running SNMP on the mobile host, the MIB (Management Information Variable) can be accessed, and the block labelled LIDS is where the component of the LIDS resides. The interface of the SNMP agent was designed in the local MIB to provide support for variable collection from both the

local LIDS and the mobile agents. The role of the mobile agents is to collect data and process them from remote hosts, specifically, the SNMP requests. They have the capability to migrate between hosts and to transfer information back to their original LIDS. On the other hand, the local LIDS agent is responsible for detecting and responding to any local intrusion, and to the events that originated from remote nodes (Albers, et al., 2002). Albers et al. suggested that the audit source for each LIDS should use SNMP auditing. They also suggested that the mobile agents should take the responsibility for transporting the SNMP messages instead of sending it over an unreliable UDP connection. Albers suggested the use of anomaly detection or misuse detection method to check against any intrusions. The LIDS should immediately communicate any known intrusion to other LIDS, in the network, which could respond by performing re-authentication, or totally ignoring the affected node, if all the LIDS decide to take cooperative action (Albers, et al., 2002).

This type of approach is not directly applicable in a wireless sensor network. However, this approach, which involves exploring localised information, could be the key to effective intrusion detection methods in a wireless sensor network (Estrin, Govindan, Heidemann, & Kumar, 1999). Effective intrusion detection in wireless sensor network is still an unresolved issue, and needs to find an effective solution.

5. Cryptography and WSN

Wireless sensors are considered as constrained devices due to obvious limitations in the number of gates, power, bandwidth, etc. Like any traditional networks, it requires protection against malicious attacks such as eavesdropping, data alteration, and packet injection. To address this problem, data cryptography has been used as a method of protecting the network. Presently, sensor networks use symmetric key cryptography, exclusively, but this approach can put the entire network at risk if one of the nodes has been compromised. The problem arises because the shared key that is supposed to be a secret is exposed. This can be overcome by using one shared key among two nodes in the network. This approach, however, does not allow new nodes to be added to the network. Thus, for a sensor network with n number of nodes, each node must possess (n - 1) number of keys. These keys must be established in the network, together with a mechanism to distribute the secure keys. Currently, the sensor devices have very limited computational power. This limitation makes it too expensive, in terms of overhead, to implement the public key cryptography in the node. For example, a parameter size of 160 bits is required to achieve 80 bits of security in ECC, which it gives the same level of security as the 1024-bit RSA. Some studies had been conducted to evaluate different parameters in regard to the feasibility of PKC in wireless sensor networks (Peter, et al., 2008). Other studies had evaluated different parameters such as the processing time, and memory requirements. Researchers have also been untaken pertaining to the use of different architectures to run PKC, effectively (Modares, 2009).

6. Conclusion

The WSN still face many security challenges. These include issues pertaining to routing, provision of QoS, efficient use of energy, sensor security, and multicasting. It is imperative that network system originators and network providers to be constantly ahead to face all the challenges and threats to embedded systems. They must constantly reassess their network security requirements and deal with new threats and attacks, effectively.

Acknowledgments:
This work was supported in part by the University of Malaya, Kuala Lumpur Malaysia under UMRG Grant (RG080/11ICT).

References

[1] Albers, P., Camp, O., Percher, J.-M., Jouga, B., Mé, L., & Puttini, R. (2002, April). Security in ad hoc networks: A general intrusion detection architecture enhancing trust based approaches. Paper presented at the First International Workshop on Wireless Information Systems (WIS-2002), Ciudad Real, Spain.

[2] Anisi, M. H., Abdullah, A. H., & Razak, S. A. (2012). Efficient Data Gathering in Mobile Wireless Sensor Networks. Life Science Journal, 9(4).

[3] Awerbuch, B., Holmer, D., Nita-Rotaru, C., & Rubens, H. (2002). An on-demand secure routing protocol resilient to byzantine failures. Paper presented at the 1st ACM workshop on Wireless security, Atlanta, GA, USA.

[4] Babaie, S., Khadem-zadeh, A., & Badie, K. (2012). Distributed Fault Detection Method and Diagnosis of Fault Type in Clustered Wireless Sensor Networks. Life Science Journal, 9(4).

[5] Bidgoli, A. M., Pajouhesh, M., & Ahmadi, M. (2011). Reliable data delivery and energy efficient aware multi-path routing protocol in wireless sensor network. Life Science Journal, 8(4).

[6] Brutch, P., & Ko, C. (2003, January 27 – 31). Challenges in intrusion detection for wireless ad-hoc networks. Paper presented at the Symposium on Applications and the Internet Workshops (SAINT'03 Workshops), Orlando, Florida.

[7] Carman, D. W., Kruus, P. S., & Matt, B. J. (2000). Constraints and approaches for distributed sensor network security (final). Glenwood, MD: Cryptographic Technologies Group,Trusted Information Systems, NAI

Labs, The Security Research Division, Network Associates.
[8] Deng, H., Li, W., & Agrawal, D. P. (2002). Routing security in wireless ad hoc networks. Communications Magazine, IEEE, 40(10), 70-75.
[9] Enck, W., Traynor, P., McDaniel, P., & La Porta, T. (2005). Exploiting open functionality in SMS-capable cellular networks. Paper presented at the 12th ACM conference on Computer and communications security, Alexandria, Virginia, USA.
[10] Estrin, D., Govindan, R., Heidemann, J., & Kumar, S. (1999, August 15 - 19). Next century challenges: Scalable coordination in sensor networks. Paper presented at the 5th annual ACM/IEEE international conference on Mobile computing and networking, Seattle, Washington, USA.
[11] Hu, Y.-C., Perrig, A., & Johnson, D. B. (2003). Packet leashes: a defense against wormhole attacks in wireless networks. Paper presented at the INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, San Francisco, California, USA.
[12] Hu, Y.-C., Perrig, A., & Johnson, D. B. (2003). Rushing attacks and defense in wireless ad hoc network routing protocols. Paper presented at the 2nd ACM workshop on Wireless security, San Diego, California, USA.
[13] Jeon, P. B. (2006). A pheromone-aided multipath QoS routing protocol and its applications in MANETs. The Pennsylvania State University, University Park, PA, US.
[14] Kalita, H. K., & Kar, A. (2009). Wireless sensor network security analysis. International Journal of Next-Generation Networks (IJNGN), 1(1), 1-10.
[15] Kavitha, D., & Haritha, D. (2011). MOBILE AGENT BASED ROUTING in MANETS–ATTACKS & DEFENCES. Network Protocols and Algorithms, 3(4), 108-121.
[16] Khan, S., Loo, K.-K., & Din, Z. U. (2010). Framework for intrusion detection in IEEE 802.11 wireless mesh networks. The International Arab Journal of Information Technology, 7(4), 50-55.
[17] Kim, H.-J., Kim, J. Y., & Choi, S.-G. (2009). A method to support multiple interfaces mobile nodes in PMIPv6 domain. Paper presented at the 2nd International Conference on Interaction Sciences: Information Technology, Culture and Human, Seoul, Korea.
[18] Krontiris, I., Benenson, Z., Giannetsos, T., Freiling, F. C., & Dimitriou, T. (2009). Cooperative intrusion detection in wireless sensor networks. Proceedings of the 6th European Conference on Wireless Sensor Networks (EWSN '09), 5432, 263-278.
[19] Liu, D., & Ning, P. (2003). Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks: North Carolina State University at Raleigh Raleigh, NC, USA.
[20] Liu, D., & Ning, P. (2004). Multilevel μTESLA: Broadcast authentication for distributed sensor networks. ACM Transactions on Embedded Computing Systems (TECS), 3(4), 800-836.
[21] Modares, H. (2009). A scalar multiplication in elliptic curve cryptography with binary polynomial operations in Galois Field. University of Malaya, Kuala Lumpur-Malaysia.
[22] Modares, H., Salleh, R., & Moravejosharieh, A. (2011, 20-22 Sept.). Overview of Security Issues in Wireless Sensor Networks. Paper presented at the Third International Conference on Computational Intelligence, Modelling and Simulation (CIMSiM) Langkawi.
[23] Mohanty, P., Panigrahi, S., Sarma, N., & Satapathy, S. S. (2010). Security Issues in Wireless Sensor Network Data Gathering Protocols: A Survey. Journal of Theoretical and Applied Information Technology, 13(1), 14-27.
[24] Muraleedharan, R., & Osadciw, L. A. (2003, March 12-14). Balancing the performance of a sensor network using an ant system. Paper presented at the 37th Annual Conference on Information Sciences and Systems (CISS), Baltimore, MD, USA.
[25] Muraleedharan, R., & Osadciw, L. A. (2006). Jamming attack detection and countermeasures in wireless sensor network using ant system. Proceedings of the SPIE Wireless Sensing and Processing, 6248(Orlando), 62480G.
[26] Noack, A., & Spitz, S. (2009). Dynamic threshold cryptosystem without group manager. Network Protocols and Algorithms, 1(1), 108-121.
[27] Perrig, A., Szewczyk, R., Tygar, J., Wen, V., & Culler, D. E. (2002). SPINS: Security protocols for sensor networks. Wireless networks, 8(5), 521-534.
[28] Peter, S., Langendorfer, P., & Piotrowski, K. (2008). Public key cryptography empowered smart dust is affordable. International Journal of Sensor Networks, 4(1), 130-143.
[29] Sahadevaiah, K., & PVGD, P. R. (2011). Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks. Network Protocols and Algorithms, 3(4), 122-140.
[30] Sharma, K., & Ghose, M. (2010). Wireless sensor networks: An overview on its security threats. International Journal of Computers and Their Applications, 1, 42-45.
[31] Sharma, P., Sharma, N., & Singh, R. (2012). A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network. International Journal of Computer Applications, 41(21), 16-21.
[32] Walters, J. P., Liang, Z., Shi, W., & Chaudhary, V. (2007). Wireless sensor network security: A survey Security in distributed, grid, mobile, and pervasive computing (Vol. 1, pp. 1-50). Boca Raton, FL, USA: Auerbach Publications, CRC Press.
[33] Wood, A. D., & Stankovic, J. A. (2002). Denial of service in sensor networks. Computer, 35(10), 54-62.
[34] Xu, W., Trappe, W., Zhang, Y., & Wood, T. (2005). The feasibility of launching and detecting jamming attacks in wireless networks. Paper presented at the Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, Urbana-Champaign, IL,USA.
[35] Yoneki, E., & Bacon, J. (2005). A survey of Wireless Sensor Network technologies. University of Cambridge, Computer Laboratory.

5/25/2013