

Malicious Node Detection by a Monitoring Mechanism in Wireless Sensor Networks

Tanveer Zia and Albert Zomaya
School of Information Technologies
University of Sydney
Email: {tanzia, zomaya}@it.usyd.edu.au

Abstract

Inherent resource limitation nature of wireless sensor networks poses unique security challenges. Cryptography is not enough and efficient to secure wireless sensor networks; it can not prevent malicious nodes and tunneling of messages to wormholes and sinkholes. In this paper we propose a monitoring mechanism to detect malicious nodes; the proposed mechanism is protected with a secure triple key management scheme. In the proposed mechanism, message sending nodes monitors if message receiving nodes have altered the message or not transmitted the message at all by building a node suspicious table and periodically broadcasting the table to its neighbors. Once a node reaches a threshold of suspicious entries, message about the presence of that node is disseminated in the entire network warning all the nodes about the presence of a malicious node. Cluster leader then isolates that malicious node hence protecting the network from malicious attacks.

1. Introduction

Wireless sensor networks are inherently limited in its processing and computing capabilities. Heterogeneous nature of sensor nodes is an additional limitation which prevents one security solution. Due to the deployment nature, sensor nodes would be deployed in environments where they would be highly prone to physical vandalism. Beside node limitations, sensor networks bring all the limitations of a mobile ad hoc network where they lack physical infrastructure, and rely on insecure wireless media.

In this paper we have introduced a mechanism of malicious node to address the unique security needs of wireless sensor networks. A malicious node detection method has been presented in [5] based on signal strength and originator's geographical position but this method assumes that sensor nodes will remain static after deployment, while in real life this is not the case. Many

applications [7, 8] introduced in literature require sensor networks to be highly dynamic. The method presented in this paper addresses the mobility of sensor nodes in a hierarchical fashion where nodes form a parent child relationship.

In our malicious node detection mechanism we consider the dynamic and scalable nature of sensor networks where sensor nodes are replaced after reaching energy exhaustion. Message sending node observes the packet receiving node hence becoming a monitor to watch the behavior of receiving node. Due to broadcast nature of wireless sensor networks the monitoring node watches if the receiving node is sending the packet intact or alters the packet contents other than adding its header information. Section 2 provides an overview of related work. In section 3 we describe the sensor network formation, leader election and route discovery process, followed by the security concerns in sensor networks in Section 4. Section 5 presents a brief overview of the secure triple key management scheme. In Section 6 we describe the malicious node detection protocol, followed by an analysis of our scheme in Section 7, and lastly in Section 8 we conclude the paper with future directions in mind.

2. Related Work

Eschenauer and Gilgor [12], present a probabilistic key pre-distribution scheme where each sensor node receives a random subset of keys from a large key pool before deployment. To agree on a key for communication, two nodes find one common key within their subsets and use that key as their shared key. Chan et al [13], extended this idea and developed three key pre-distribution schemes; q-composite, multipath reinforcement, and random-pairwise keys schemes.

Pietro et al [14], Present a random key assignment probabilistic model and two protocols; 'direct and cooperative' to establish a pairwise communication between sensors by assigning a small set of random keys to each sensor. This idea later converges to pseudo

random generation of keys which is energy efficient as compare to previous key management schemes.

Liu and Ping [15] present a general framework for establishing pairwise keys between sensors on the basis of a polynomial-based key pre-distribution protocol (Blundo et al 1993) then they present two instantiations of the general framework: a random subset assignment key pre-distribution scheme, and a hypercube-based key pre-distribution scheme. Finally, they present a technique to reduce the computation at sensors so that their schemes can be implemented efficiently.

Du et al [16] pairwise key pre-distribution is an effort to improve the resilience of the network by lowering the initial payoff of smaller scale network attacks and pushes adversary to attack at bigger scale to compromise the network. Later in their work Du et al [17] present a key scheme based on deployment knowledge. This key management scheme takes advantage of the deployment knowledge where sensor position is known prior to deployment. Because of the randomness of deployment, it is not feasible to know the exact neighbor locations, but knowing the set of likely neighbors is realistic, this issue is addressed using the random key pre-distribution of Eschenauer and Gilgor [12].

Zhu et al [18] have presented LEAP; a security mechanism having a key management scheme based on a set of four keys for each sensor node which restricts the security impact of a node to the immediate neighborhood of the compromised node.

Marti et al [19] have proposed watchdog and pathrater tools to detect and mitigate routing behavior, where watchdog detects a misbehaving node, however, the listed weaknesses such as ambiguous collisions, limited transmission power, false misbehavior and collusions make this technique less effective.

3. Network Formations, Leader Election and Route Discovery

Wireless Sensor networks are consisting of large number of tiny sensors and actuators with limited energy, computations and transmission power [4, 7]. Sensor nodes are randomly deployed in an environment where they are prone to physical interaction and most likely left unattended after deployment. Although nodes have many limitations but they report to a single destination called base station which is believed to be a powerful computer safely located with large computation resources.

We consider a hierarchical topology of sensor networks where sensor nodes form a parent child relationship in clusters [1, 2] when deployed. In this topology nodes broadcast their IDs and listens to the neighbors, add the neighbor IDs in its routing table and count the number of neighbors it could listen to. Hence these connected neighbors become a cluster. Each cluster elects a sensor node as a leader. All inter-cluster communication is routed through cluster leaders. Cluster leaders also serve as fusion nodes to aggregate packets and send them to the base station. Cluster leader and its neighbor nodes form a parent-child relationship in a tree-based network topology. A cluster leader receives highest number of messages, this role changes after reaching an energy threshold, hence giving opportunity to all nodes becoming a cluster leader when nodes move around in a dynamic environment. Coverage of cluster depends on the signal strength of the cluster leader. Cluster leader and its neighbor nodes form a parent-child relationship in a tree-based network topology. In this multi hop cluster model, data is collected by the sensor nodes, aggregated by the cluster leader and forwarded to the next level of cluster leader, eventually reaching the base station. Figure 1 below shows a network of 100 nodes forming 5 clusters. Nodes 1, 2, 3, 4 and 5 are the cluster leaders in this topology [1].

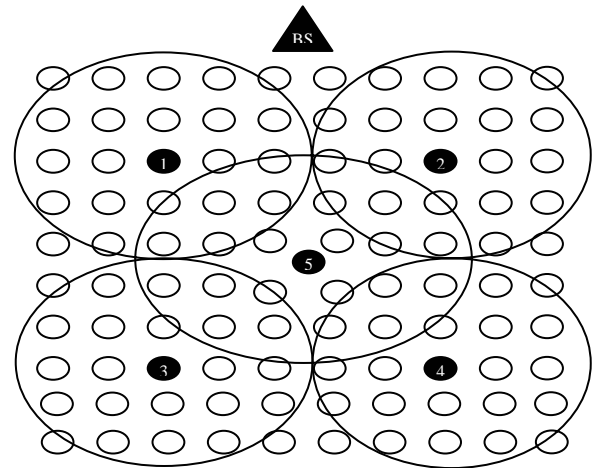


Figure 1. Network formation and cluster leader election. Nodes 1, 2, 3, 4, 5 are the cluster leaders and BS is the base station.

4. Security Concerns in Wireless Sensor Networks

Ideally any network should meet the security goals of CIAA – Confidentiality, Integrity, Authentication and Access control [6]. *Confidentiality* means ensuring a message remains concealed from any attack, *integrity* refers to the trustworthiness of message that it has not

been tampered with, *authentication* is confirming that the message is from the node where it claims to be from and *access control* is the ability to determine if a node has access to the right resources. Two major reasons why wireless sensors networks are posing unique security challenges are (1) node constraints: energy, processing power and memory limitations, and (2) network constraints: wireless and ad hoc nature of network. Table I below summarizes possible attacks [3] on wireless sensor networks.

Table 1. Summary of Attacks on Wireless Sensor Networks

Attacks	Attack description
Spoofed, altered, or replayed routing information	Create routing loop, attract or repel network traffic, extend or shorten source routes, and generate false error messages etc
Selective forwarding	An adversary selectively forwards the packets. A malicious node act like a black hole and refuses to forward every packet it receives.
Sinkhole attacks	Attracting traffic to a specific node, e.g. to prepare selective forwarding
Sybil attacks	A single node presents multiple identities, allows to reduce the effectiveness of fault tolerant schemes such as distributed storage and multipath etc.
Wormhole attacks	Tunneling of messages over alternative low-latency links to confuse the routing protocol, creating sinkholes etc.
Hello floods	An attacker sends or replays a routing protocols hello packets with more energy

We have presented a security framework for wireless sensor networks [1] to provide desired security countermeasures against these attacks. Our security framework consists of three interacting phases: cluster formation, a secure triple key management [2] and secure routing schemes. In this paper we have focused on detection and isolation of a malicious node. We intend to address the unique security challenges in sensor networks one by one and these solutions will become part of our broader security framework eventually.

In our mechanism we have specifically addressed wormhole and sinkhole attacks [3, 4, 5]. If an adversary is able to compromise a node closer to the base station it can disrupt the routing by creating a wormhole and tunneling all the traffic towards a sinkhole. Detection of wormhole attacks is difficult if they are used together with selective forwarding and Sybil attacks. The malicious node detection protocol is safe guarded by our

secure triple key management scheme. Next section briefly discusses this scheme.

5. Secure Triple-Key Management Scheme

Our secure triple-key management scheme¹ is consisting of three keys: two pre-deployed keys in all nodes and one in-network generated cluster key for a cluster to address the hierarchical nature of sensor network.

K_n (network key) – Generated by the base station, pre-deployed in each sensor node, and shared by the entire sensor network. Nodes use this key to *encrypt* the data and pass onto next hop.

K_s (sensor key) – Generated by the base station, pre-deployed in each sensor node, and shared by the entire sensor network. Base station uses this key to *decrypt* and process the data and cluster leader uses this key to *decrypt* the data and send to base station.

K_c (cluster key) – Generated by the cluster leader, and shared by the nodes in that particular cluster. Nodes from a cluster use this key to *decrypt* the data and forward to the cluster leader. Nodes will use this key only when they are serving the purpose as a cluster leader, otherwise nodes will not need to decrypt the message received from other nodes thus saving the energy and processing power.

This secure triple-keys management scheme is a much resilient solutions against many of sensor network attacks. We describe below how this scheme works:

Following notations have been used in our key management scheme.

ID#	A unique ID of the sensor node
TS	An encrypted time stamp for beacon authentication
S	Seed value randomly generated by the base station
Aggr message	Aggregated message by a cluster leader
CL	Cluster leader – a node randomly elected as a leader for a given group of sensors through a leader election process
BS	Base station, a node assumed to be very powerful with extra ordinary computation resources
$MAC_k(m)$	Message authentication code for message m, generated using key k
Level	Level of node – value indicate the number of hops between the base station and node

¹ A naïve idea about this scheme was presented in INFOCOM 2006 student workshop [20]

5.1 Base station to node key calculation

Base station uses K_n to encrypt and broadcast data. When a sensor node receives the message, it decrypts it by using its K_s . This process follows as: Base station encrypts its own ID, a current time stamp TS and its K_n as a private key. Base station generates a random seed S and assumes itself at level 0. Here S is a pseudo-random function [11] known to the base station only. The packet contains following fields:

K_n	MAC	ID	TS	S	message	Level 0
-------	-----	----	----	---	---------	---------

Sensor node decrypts the message received from the base station using K_s . Here MAC is message authentication code for a message (m).

5.2 Nodes to Cluster leader key calculation

When node sends a message to cluster leader, it constructs the message as follows:

$$\{ID_{sn}, K_n, TS, MAC, S(\text{message})\}$$

Cluster leader checks the ID from the packet, if the ID in the packet matches the ID it holds, it verifies the authentication and integrity of the packet through MAC. Otherwise, packet is dropped by the cluster leader. Node builds the message using the fields below:

K_n	MAC	ID	TS	S	message	Level 2
-------	-----	----	----	---	---------	---------

5.3 Cluster leader to next hop cluster leader key calculation

Cluster leader aggregates the messages received from its nodes and forwards it to next level cluster leader or if the cluster leader is one hop away from the base station, it directly sends the message to the base station. Receiving cluster leader checks its routing table and constructs the following packet to be sent to next level cluster leader or to the base station. Cluster leader adds its own ID CL_n , its network and cluster key in incoming packet and rebuilds the packet as under:

$$\{ID, K_{CLn}, [ID_{sn}, K_n, TS, MAC, S(\text{Aggr message})]\}$$

K_n	K_c	MAC	ID	TS	S	Aggr message	Level 1
-------	-------	-----	----	----	---	--------------	---------

Here ID is the ID of receiving cluster leader which wraps the message and sends it to the next hop cluster leader or to the base station if directly connected. Next hop cluster leader receives the packet and checks the ID, if the ID embedded in the packet is same as it holds, it

updates the ID for the next hop and broadcast it, or else the packet is discarded. *Aggr message* refers to the message aggregated by the cluster leader.

5.4 Cluster leader to base station key calculation

Base station receives the packet from its directly connected cluster leader; it checks the ID of sending cluster leader, verifies the authentication and integrity of the packet through MAC. Cluster leader directly connected with base station adds its own ID along with the packet received from the sending cluster leader. Packet contains the following information:

$$\{ID_{CL2}[ID_{CL1}, K_n, [ID_{s2}, K_n, TS, MAC, S(\text{Aggr message})]]\}$$

Figure 2 below illustrates the key calculation process from nodes to base station.

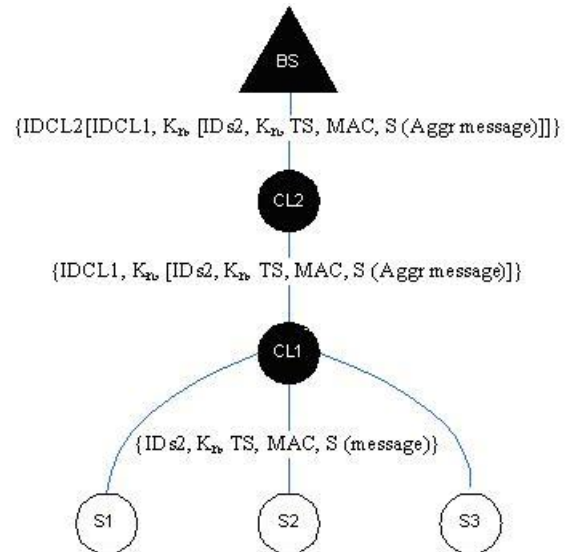


Figure 2. Key calculation from Sensor Node S2 to Cluster Leader CL1, Cluster Leader CL1 to Cluster Leader CL2, and Cluster Leader CL2 to the Base Station BS

6. Malicious Node Detection Mechanism

A malicious node is a compromised node where an adversary has some how able to break the encryption [4] and has got access to the secure keys and routing protocols of the sensor network. Malicious node detection mechanism is protected by our underlying security framework having a set of three secure keys as discussed in section IV. This section demonstrates how a malicious node is detected if in a less likely event of

secure triple key management scheme compromise. In figure 3 a routing path has been formed from cluster leader 4-5-2-BS.

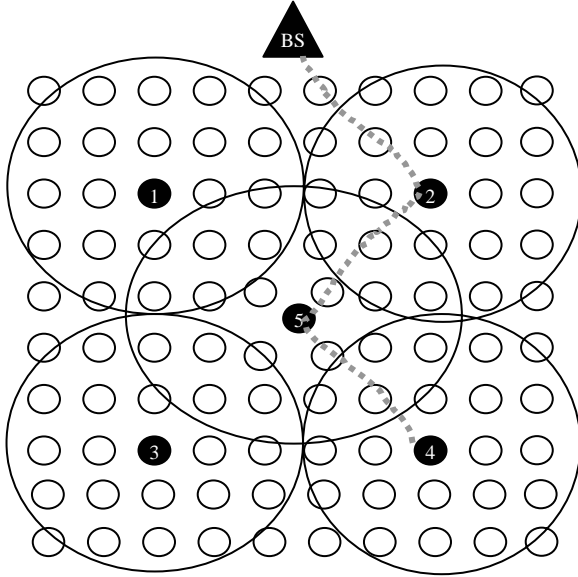


Figure 3. Routing path establishment

In our malicious node detection technique we use a monitoring mechanism. In this mechanism when a node A sends message to node B , it converts itself to a monitoring mode we refer here as A_m . Due to the broadcast nature of wireless sensor networks A_m monitors the behavior of node B after sending the message. When node B transmits the message to the next node, A_m hears that and compares with the message it has sent to node B , hence establishing *original* and *actual* message. If the message transmitted by node B is *original* then node A_m ignores it and continues with its own tasks but if there is a difference between *original* and *actual* messages greater than a threshold, the message is considered as suspicious and node B is now considered as a suspicious node B_s .

Each node builds a *node suspicious* table containing the reputation of nodes in the cluster. Entries in this table contain the node ID, and the number of suspicious and unsuspecting entries. Nodes update this table every time it identifies a suspicious activity by increasing suspicious count by one for that particular node. In Table II below ID is the unique ID of sensor node; NS denote node suspicious and NU node unsuspecting entries.

Table 2. Node Suspicious Table

Node ID	Suspicious entries	Unsuspecting entries
ID	$NS > 1$	$NU > 1$

All the nodes locally build a *node suspicious* table. Every time A_m identifies a suspicious entry it adds into its node suspicious table and disseminate this information among neighbors and all the nodes listening to this message update their *node suspicious* table. This broadcast message also act as an inquiry, nodes listening to this message reply with their opinion about B_s . In the Figure 4 Nodes C and D are neighboring nodes of A_m and B_s , they listen the transmission from B_s and respond with suspicious entry if the suspicious count for B_s in its node suspicious table is greater than its unsuspecting count, otherwise it responds with unsuspecting. Figure 5(a) shows a message sent by Node A , secured with our network key K_n and in Figure 5(b), an altered message is shown from Node B .

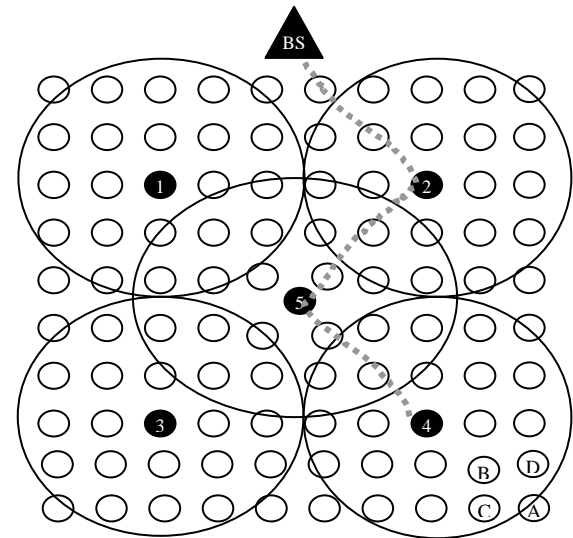
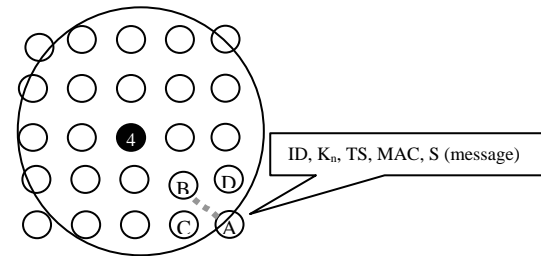


Figure 4. Node A_m (monitoring node) B_s (Suspicious node) and Nodes C & D neighboring nodes.

ID, K_n , TS, MAC, S (message)



(a)

ID, K_n , TS, MAC, S (altered message)

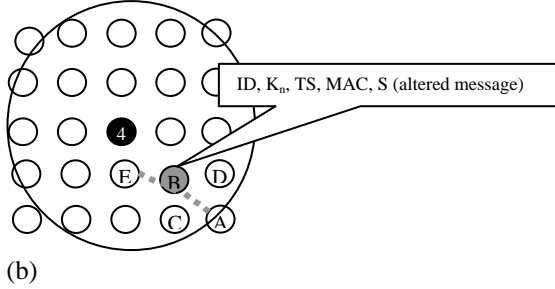


Figure 5. (a) Message sent by Node A (b) Message altered by Node B:

Here ID is the node's unique identifier, K_n is the network key, TS is an encrypted time stamp, MAC is the message authentication code generated using K_n for message m and S is the randomly generated seed value by the base station.

Node A_m collects the replies from neighbors and updates its *node suspicious* table; it increases its own suspicious entry for B_s by one and the unsuspecting entries accordingly.

Once the *suspicious* entries reach a threshold, node A_m broadcasts that node B_s is a *suspicious* node and all the neighboring nodes update their *node suspicious* tables that a malicious node is present in the cluster. When the presence of a *suspicious* node message reaches a Cluster Leader, it isolates B_s by erasing B_s ID from its *nodes table* and discards any message coming from B_s . Cluster leader broadcasts the message that node B_s has been isolated, therefore any message originated from B_s is discarded by its neighboring nodes hence isolating node B_s from the network.

7. Analysis of Proposed Solution

The proposed protocol can be used to detect a malicious node in wireless sensor networks depending on two factors: *nodes density* and the *transmission power*. Nodes density determines the number of neighbors a malicious node will have and detection of malicious activity by the neighboring nodes. Transmission power refers to the ability of a node to actively receive and send *suspicious* entry when a malicious node is detected in its neighborhood. Given the resource starved nature of sensor nodes there is tradeoff between malicious node detection and energy being consumed in more frequent *suspicious* and *unsuspicious* messages. We make an assumption that sensor networks would be secured with the use of our triple key management scheme and the probability of a node compromise is very low in the presence of our security framework. In an unlikely event

of a malicious node presence, our malicious node detection mechanism presented in this paper will provide an added resilience against wormhole and sinkhole attacks. In a typical transmission by a sensor node we assume a packet size of 44 bytes having following fields:

IDs	Keys	TS	S	Data	MAC
(3)	(3)	(1)	(1)	(0..31)	(4)

Taking into account 128K program memory of ATmega128L MICA2Dot [10] our framework can be best implemented in a network of up to 3000 sensor nodes. Going beyond this number may require a tradeoff between the security and performance. Assuming the ongoing developments in enhancing the program memory this mechanism will be feasible in even larger and denser networks.

The mechanism presented here takes into consideration the nodes and cluster leaders which are not participating in sending and aggregating the data. These nodes forward the data packets without applying any further cryptographic operation, thus further saving the processing power and memory.

We consider TinySec [9] as a bench mark for our research and compare our security mechanism with it. TinySec is so far the de facto security solution at Berkeley. Table III below compares the TinySec and the packet size used in our node detection mechanism. This comparison shows that our node detection mechanism do not have any additional overheads, instead it overcomes the weaknesses in existing security solutions in sensor networks.

Table 3. Comparison of Overheads in TinySec and Node Detection Mechanism

	Application Data (b)	Packet Overhead (b)	Total Size (b)	Time to transmit (ms)	Increase over TinyOS stack
Current TinyOS Stack	24	39	63	26.2	--
TinySec-Auth	24	40	64	26.7	1.6%
TinySec-AE	24	44	68	28.3	8%
Node detection mechanism	24	44	68	28.3	8%

8. Conclusion and Future Work

We have presented malicious node detection protocol by a monitoring mechanism in wireless sensor networks supported by a set of secure triple key management scheme to protect the sensor networks from the attacks raged by adversaries. With our thorough analysis we believe our malicious node detection protocol is much resilient against attacks listed in Table 1 and is applicable without any additional packet overheads than what has been proposed in literature. We intend to develop a broader security framework to provide a comprehensive security solution against the attacks in sensor networks. Our future directions are to investigate node localization issues and testing our security framework through rigorous experimentation and simulation.

References

- [1] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," IEEE Proceedings of the 33rd Hawaii International Conference on System Sciences, Jan. 2000, pp. 1–10.
- [2] M. Tubaishat, J. Yin, B. Panja, S. madria, "A Secure Hierarchical Model for Sensor Networks", ACM SIGMOD, Volume 33 , Issue 1 March 2004, ACM Press, NY
- [3] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", University of California at Berkeley, USA 2003.
- [4] I. Khalil, S. Baghi, and C. Rotaru, "DICAS: Detection, Diagnosis and Isolation of Control Attacks in Sensor Networks", IEEE Securecomm 2005, 5-9 September 2005, Athens Greece.
- [5] W. Junior, T. Figueiredo and H. Wong, "Malicious Node Detection in Wireless Sensor Networks", Proceedings of the 18th International Parallel and Distributed processing Symposium (IPDPS'04), April 26-30 2004, Santa Fe, New Mexico.
- [6] C.P. Pfleeger, and S.L. Pfleeger, "Security in Computing" 3rd edition, 2003, Prentice-Hall Inc. NJ
- [7] C.Y. Chong, and S.P. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges", IEEE 2003
- [8] S.H. Choi, B.K Kim, J. Park, C.H. Kang, D.S. Eom "An Implementation of Wireless Sensor Networks", IEEE Transactions on Consumer Electronics Vol. 50, Issue 1, Pages 236-244, Feb. 2004
- [9] C. Karlof, N. Shastri and D. Wagner, "TinySec: A Link layer Security Architecture for Wireless Sensor Networks", SenSys'04, November 3-5 2004, Baltimore, Maryland, USA
- [10] Crossbow Technologies Inc. <http://www.xbow.com/> Viewed on 14 August 2006
- [11] O. Goldreich, S. Goldwasser, and S. Micali, "How to Construct Random Functions. Journal of the ACM, Vol. 33, No. 4, 1986, pp 210-217.
- [12] L. Eschenauer and V. Gligor, "A Key-management Scheme for Distributed Sensor Networks", Proceedings of the 9th ACM conference on Computer and Communication Security 2002, Washington DC, USA
- [13] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks". In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, California USA
- [14] R. Pietro, L. Mancini, and A. Mei, "Random key-Assignment for Secure Wireless Sensor Networks", ACM SANS 2003.
- [15] D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks", ACM CCS 2003.
- [16] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks", ACM CCS 2003.
- [17] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge", IEEE InfoCom 2004.
- [18] S. Zhu, S. Setia and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", ACM Conference on Computer and Communications Security (CCS '03), October, 2003.
- [19] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", In the proceedings of 6th Annual International Conference on Mobile Computing and Networking (MobiCom 2000), pages 255-265, Boston, AM, ACM Press, August 2000
- [20] T.A. Zia, and A.Y. Zomaya, "A Secure Triple-Key Management Scheme for Wireless Sensor Networks", In the proceedings of the IEEE INFOCOM 2006 Students Workshop, April 23-24, 2006, Barcelona, Spain