A Secure Message Percolation Scheme for Wireless Sensor Network

Md. Abdul Hamid[1] and Choong Seon Hong[1]

[1]Networking Lab, Department of Computer Engineering, Kyung Hee University
1 Seocheon, Giheung, Yongin, Gyeonggi, 449-701 South Korea
hamid@networking.khu.ac.kr and cshong@khu.ac.kr

Abstract. Wireless Sensor Network (WSN) deployed in hostile environments suffers from severe security threats. In this paper, we propose a Secure Message Percolation (SMP) scheme for WSN. We engineer a secure group management scheme for dealing with data gathered by groups of co-located sensors and analyze the robustness against increasing number of compromised sensor nodes. Key pre-distribution is performed with the concept of star key graph where one sensor node dominates other nodes. Analytical result shows that our protocol is robust against node compromise and scales well and needs a few pre-distributed shared keys per node.

Keywords: Secure Group, Node Compromise, Robustness, Star Key Graph.

1 Introduction

Lightweight secure protocol for resource-constrained WSN is challenging and much works are going on in designing storage and computationally inexpensive mechanism [2] [3] [16]. We consider few important issues in engineering our security protocol. Firstly, key storage for individual sensor node needs to be reasonably small. For example, if there are N nodes in the network, then we can not expect that a node can store $N - 1$ keys to share a secrete key with each of the other nodes. Secondly, in case where quite a good amount of sensor nodes are compromised by an adversary, the communications among other nodes should still be secure. Thirdly, it should be ensured that both local and global connectivity is maintained. A sensor node should be able to securely communicate with its local neighbors (i.e., sensor physically located within transmission range). Connectivity among local zones should provide global network connectivity [14]. Finally, asymmetric cryptography to WSN is too expensive, because they require expensive computations and long messages that might easily exhaust the sensor's resources [13]. That's why we take symmetric cryptographic operations and spread the load across network in a distributed fashion. We take into consideration secure network formation (bootstrap), data aggregation by

This work was supported by MIC and ITRC Project. Dr. Choong Seon Hong is the corresponding author.

groups of locally co-located nodes and rekeying. Key management and rekeying are basically performed in a distributed fashion to aiming at proposing a more lightweight load for individual sensors. We analyze our scheme's robustness against node compromise when adversary compromises network nodes. We also show that our protocol scales well and needs a few pre-distributed shared keys per node.

Rest of the paper is structured as follows. Section 2 outlines the network assumptions and preliminaries; Section 3 presents our scheme in details. We analyze our SMP scheme in Section 4. Related works and comparisons are noted in Section 5 and Section 6 concludes the paper.

2 Network Assumptions and Preliminaries

Our network is a multi-hop in nature supporting node deletion/addition. We consider a heterogeneous network, where two types of sensors are deployed: ordinary sensor node (SN) and group dominator (GD). SN is simple, inexpensive and stringent in resources (power, memory and computation), while GD is rich is resources and more compromise-tolerant. We also assume that one GD can communicate with its neighbor GD to forward aggregated messages towards base station. There is no communication link among SNs within one group and between SNs in different group (Fig. 1b).

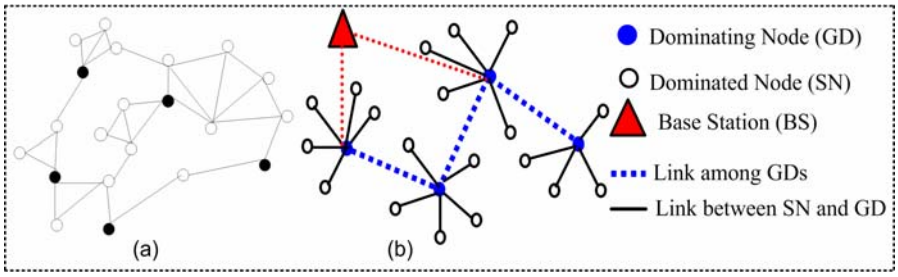


Fig. 1. (a) WCDS. (b) Star based-WCDS for proposed SMP scheme.

We assume that once the sensors are dispersed over the area of interest, they remain relatively static. We consider the sensors in the whole network as a graph G = (V, E), where V is the set of sensors in the network and E is the set of direct communication links. A direct communication link is present between SNs and its corresponding GDs if and only if they are within the transmission range of one another and share the same key. In such a setting, we apply our scheme to form a network-wide star based weakly connected dominating set (SWCDS) (Fig. 1b). A weakly connected dominating set (WCDS), S_W, is a dominating set where the graph induced by the stars of the vertices in S_W is connected. A star of a vertex comprised of the vertex itself and all the ordinary sensor nodes adjacent to it (all the black nodes in Fig. 1a). The underpinning of our proposed scheme is the star based weakly connected dominating set. In fact, it is easy to see that each dominating node (or vertex) in the SWCDS is at the center of a star (Fig. 1b). Thus for each dominating node in a SWCDS of the overall network,

we have one star where all the other nodes in the star are just one hop apart. For the space constraint, we request the readers to look at references [1] and [14] for details about dominating set, connected dominating set and WCDS.

3 Proposed SMP Scheme

In our approach, key pre-distribution is performed using the concept of star key graph [17]. This is the special class of a secure group where each sensor node has only three keys to maintain: its individual key (shared between SN and GD), and a local group key that is shared by every user in the star graph with their corresponding GD and a pairwise key between SN and BS. BS stores all the keys of SNs and GDs. We use the notations in table 1 to describe our scheme.

Table 1. Notations used in SMP scheme

Notation	Definition
i ($0 \le i \le N$)	Ordinary sensor node i (SN_i)
j ($0 \le j \le Y$)	Group dominator j of ordinary sensor i (GD_j)
ID_i	ID of the ordinary sensor node i
ID_j	ID of the group dominator j
K_{Gj}	Group key shared by all sensors in a group j and GD_j
$K_{(SNi,GDj)}$	Pairwise key between a sensor i and GD_j
$K_{(SNi,B)}$	Pairwise key between sensor i and Sink/BS
$K_{(GDj,B)}$	Pairwise key between GD_j and Sink/BS
M_i	Event sensed by SN_i
M_{GDj}	Message aggregated by GD_j
MAC(K,M)	Computation of Message Authentication Code of message M using key K
E(K,M)	Encryption of message M using key K
X|Y	Concatenation of X and Y

3.1 Pre-deployment Key Pre-distribution and Rekeying

Key pre-distribution: In the offline key pre-distribution phase, we assign the group keys and individual keys to a group of nodes. For this, the key assignment is accomplished according to Fig. 2a. Each GD holds group key and all individual keys. Each SN holds group key and its individual key shared with GD. In this phase, all the SNs are also assigned unique ID_i ($1 \le i \le N$) which are also stored by the respective GDs. Each GD is also assigned ID_j ($1 \le j \le Y$), where Y is the total number of group dominators in the network.

Rekeying: During the offline key pre-distribution, all the nodes are assigned the keys but not all the nodes are deployed. When any of those remaining nodes is deployed, it sends the JOIN_REQ_NEW message using its own individual key. If authorized by the access list of GD, it joins the group. Otherwise, GD forwards this to BS. BS informs GD about the individual key of that SN. If authenticated by BS, GD generates a new group key and encrypts the new group key with the newly added node's individual key and sends it to the SN. All other nodes in the group know about the change by a multicasting by the GD of that group. For leaving a star graph, the node simply leaves a message to inform the GD which in turn generates a new group key and unicasts it within the group members (Fig. 2b). For example, let's say, SN_4 in

Fig. 2b wants to join the existing group in the figure shown above. GD changes the group key K_G to a new key K_{Gnew}, and sends the following rekeying messages:

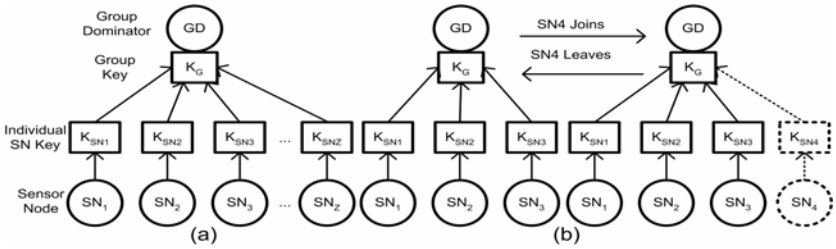


Fig. 2. (a) Pre-distribution of secret keys using star key graph. (b) Rekeying.

$GD_j \rightarrow$ *all* SN_i**:** $E_{K_G}(K_{Gnew})$, Encrypted new group key with the old group key.

$GD \rightarrow SN_4$**:** $E_{K_{SN4}}(K_{Gnew})$, Encrypted new group key with the joining SN's individual key.

Similarly, when any SN wants to leave the group, it just sends a leave message. GD deletes the leaving SN and updates the K_G to new K_{Gnew} and unicasts the following message:

$SN_4 \rightarrow GD$**:** E_{KSN4}(leave), SN_4 wants to leave the group.

$GD \rightarrow SN_{i-1}$**:** $E_{KSNi-1}(K_{Gnew})$, GD unicasts the new group key encrypted with remaining SN's individual key.

3.2 Post Deployment Phase

Ordinary sensor nodes and group dominators having the offline pre-distributed secret keys are deployed over the area of interest. In this section we describe secure bootstrap (network formation), data aggregation and rekeying. For convenience, we have described rekeying mechanism in section 3.1.

3.2.1 Secure Network Formation.

It has been shown in [15] that sensors belonging to the same group can be deployed close to each other without the knowledge of sensor's expected location. Considering the fact in [15], we describe secure network formation with exception handling (e.g., a SN does not belong to same group).

After the deployment, each SN_i discovers its own GD_j. For this purpose, SN_i multicasts an encrypted JOIN_REQ (using individual key K_{SNi}) message to all of the nodes within its transmission range. If the corresponding GD_j is within its transmission range (i.e., one hop distance), it gets the message and decrypts it as all the individual keys of the sub-ordinate nodes are known to the GD_j. Upon successful decryption of the message, the GD sends a JOIN_APRV message to the SN_i encrypting it with the group key. Thus the SN_i becomes a dominated node of a corresponding GD_j. If, for any SN_i, the GD_j assigned during pre-distribution of keys, is not within one hop distance; the SN_i needs to inform the BS for resolving the issue.

We term this SN as the 'Orphan' (SN_{ORP}). On discovering itself as an Orphan the SN_i sends a GD_ERR message encrypting it with its individual key. This message is simply forwarded by other sensors in the network to reach to the BS. For resolving the unexpected issue of Orphans we consider two special cases.

Case I. The orphan has no dominator as its one-hop neighbor. In such a case, after getting the GD_ERR message from the Orphan, the BS issues a command to assign the role of a GD to the Orphan. For sending the command, the BS uses the individual key of the Orphan. This newly formed GD does not have any other dominated SN nevertheless; employing this method keeps the isolated node connected with the rest of the network.

Case II. The Orphan does not have its own GD within its one-hop neighborhood but a GD of another group is present in the vicinity. Failing to find out its own GD, SN sends the encrypted GD_ERR message to the BS. Now, as the GD of another group is present within its one hop distance, it eventually gets the encrypted GD_ERR message (only detects the type of message and just notes this incident) and informs this 'Orphan Information' using ORP_ERR (encrypted with its group key) to the BS. The BS eventually gets two separate but interrelated reports; one from SN_{ORP} and another from the neighboring GD. The BS checks whether both these reports tell about the same SN_{ORP} or not. If same SN_{ORP}, BS issues a command to that neighbor GD to be its adopter and also sends the individual key for the SN_{ORP}. The GD in turn uses this key to send its K_G to the SN_{ORP} to welcome it in its own group. Thus, all the stars could form a weakly connected network where the GDs of the logical groups (stars) are the dominating nodes and all other nodes in the network are dominated (Fig. 1b).

3.2.2 Secure Data Aggregation

Once the network is logically structured as a weakly connected dominating set, the sensory data from the sensors can be transmitted securely to the BS. GDs are responsible to aggregate data collected from different sensors. If there are Z number of ordinary sensors (SN) in a group, for fidelity and correctness of data, the GD waits for the same sensing event from at least q ($q \leq Z$) number of the SNs, where q is the threshold value set for a particular group.

We consider any one group with ordinary SNs and its corresponding GD. Once an event occurs, q out of Z ($0 \leq q \leq Z$) ordinary sensors (ID_1, ID_2, . . ., ID_q) within the sensing area detect the event and send information to the GD.

$$SN_i \rightarrow GD_j : ID_i|E(M_i|MAC(M_i, K_{(SNi,GDj)}), K_{(SNi,GDj)}))$$

Upon receiving the message sensed by SN_i (ordinary sensor), Dominator GD_j verifies every single MAC and generates an aggregated report (and discards the false packet if any). GD broadcasts the aggregated results M_{GDj} and MAC to all sensors.

$$GD_j \rightarrow all\ SN_i : ID_{GDj}|M_{GDj}|MAC(M_{GDj}, K_{Gj})$$

All SNs in a particular group j verifies the aggregated report whenever they receive it for the consistency with its own sensed event. It creates a MAC only to be verified by the Sink (BS) but to be relayed by its GD. The message format is

$$SN_i \rightarrow GD_j : ID_i|MAC(K_{(SNi,B)},ID_i|M_{GDj})$$

Now, GD collects all the MACs from ordinary sensor nodes and sends q MACs, q IDs, ID_{GDj}, and M_{GDj} to the sink directly or via its neighboring GD (multi-hop path through consecutive GDs towards the Sink) as follows

$$GD_j \rightarrow Sink\text{:}\ ID_{GDj}, E(K_{(GDj,B)}, ID_{GDj}|M_{GDj}|ID_1|MAC_{(SN1,B)}|.....ID_q|MAC_{(SNq,B)})$$

The q MACs and aggregation report M_{GDj} are sent securely to the base station. Upon receiving an aggregation report, the sink first decrypts the message using the corresponding key $K_{(GDj,B)}$, then it checks whether the report carries at least q distinct MACs from ordinary sensors and whether the carried MACs are the same as the MACs it computes via its locally stored keys. If no less than q MACs is correct, the event is accepted to be legitimate; otherwise it is discarded.

4 Analysis

In our scheme, we form a probable star based WCDS to cover almost all of the nodes in the network with minimum effort. As shown in Fig.1b, SWCDS requires less number (or equal to) of dominating nodes to cover the whole network than that of a connected dominating set (CDS) requires [14]. We use the distinct group keys for each of the GDs and distinct individual keys for each SN. So, the number of individual keys required for our network is much less than other probabilistic key management schemes. Table 2 shows the overhead of our scheme. We assume the length of ID, key and MAC is 2, 16 and 4 bytes respectively. We consider *20* ordinary sensor nodes in one group and an aggregated report travels 10 hops on an average. We calculate the overhead based on the message format described in section 3.2.2.

Table 2. Overhead of secure message percolation scheme (Excluding encryption)

Overhead Type	SN	GD
Storage	48 bytes (3 keys)	352 bytes (1+1+Z keys)
Communication	12 bytes (2 ID + 2 MAC)	1220 bytes ((1 ID_{GD} + (1 ID_{sn} + 1 MAC) Z) H hops)
Computation	3 MACs	21 MACs (1 MAC_{GD} + Z MAC_{SN})

4.1 Security Analysis

Our scheme ensures that, each of the GDs and the corresponding SNs can directly form the groups or stars maintaining the security of the network from the bootstrapping state. As encryption is used for message-transmission within the network from the very beginning of the network, our scheme can successfully defend Hello Flood Attack [2] and most of other attacks in wireless sensor networks. We contemplate security analysis of our scheme from various perspectives as described below.

*Ordinary sensors (SNs) are captured***:** A compromised ordinary sensor in particular group may produce an invalid MAC by providing wrong guarantee for an aggregated report. The SMP scheme is robust against this kind of attack as long as no more than q sensors within a local group are compromised. Since we devise our scheme where each aggregated report carries q number of MACs from ordinary sensors. Only the

base station checks the correctness and no less than q correct MACs from ordinary sensors is accepted by the base station. A compromised ordinary sensor may forge false event's information with valid MAC to its GD. We argue that a single faulty value will not hamper the aggregated result.

A GD is captured: When a GD is captured, it may fabricate a report. But to do that, at least q MACs need to be forged. The probability that at least q out of Z MACs is correct is given by

$$p_{GD} = \sum_{j=q}^{Z} \binom{Z}{q} p^{q} (1-p)^{Z-q}$$

where, $p=1/2^{L}$ and L is the MAC size in bits. We claim that this probability is negligible; moreover, only one group out of entire network is in fact affected while other groups are not hampered.

Both GD and ordinary SNs are captured: We consider the situation where an adversary has compromised GD and some number x ($0 \leq x \leq q$) ordinary sensor nodes. To inject a false report, GD needs at least q valid MACs. Since GD has to forge $(q-x)$ more MACs, the probability that $(q-x)$ out of $(Z-x)$ is valid, is given by

$$p_{GD}^{x} = \sum_{j=q-x}^{Z-x} \binom{Z-x}{j} p^{j} (1-p)^{Z-x-j}$$

Again, this probability is almost negligible. If an individual key is compromised, the attacker at best could send false report to the GD but when any message from the GD comes encrypted with the group key, it cannot decrypt it. So, for successful attack, it needs both the individual and group key at the same time. Moreover, compromising one key doesn't affect the rest of the keys used among other nodes and links in the network.

Network-wide Compromise of SNs and GDs: We analyze the robustness of our scheme when an adversary has randomly compromised Q ordinary SNs and j ($0 \leq j \leq Y$) GDs from the entire network. Let $p(j,q)$ be the probability that j^{th} GD (i.e., j^{th} group) having q ($0 \leq q \leq Z$) SNs compromised, we get

$$p(j,q) = \frac{\binom{Z}{q}\binom{N-Z}{Q-q}}{\binom{N}{Q}}$$

We define $g_{j,q}$ as: $g_{j,q} = 1$ if q ordinary SNs are compromised in j^{th} group and 0 otherwise. And let G_q denote the number of groups having q ordinary SNs compromised, we get

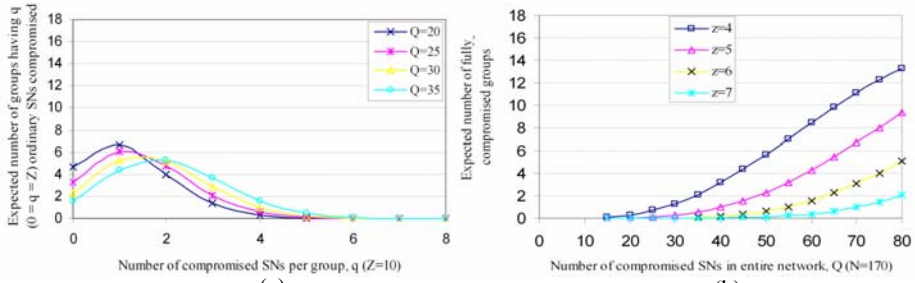
$$G_q = \sum_{j=1}^{Y} g_{j,q}, \quad \text{and}$$

$$E\left[\sum_{j=1}^{Y} g_{j,q}\right] = \sum_{j=1}^{Y} E[g_{j,q}] = Y.E[g_{j,q}] = Y.p(j,q) = Y.\frac{\binom{Z}{q}\binom{N-Z}{Q-q}}{\binom{N}{Q}}$$

Next, we assume that an adversary has compromised some groups having the z ($z \geq q$) SNs compromised and we call this situation as full group compromise. Let X be the number of fully compromised groups from entire networks. We can compute $E[X]$ by the following equation:

$$E[X] = \sum_{q=z}^{Z} G_q = \sum_{q=z}^{Z} Y \cdot \frac{\binom{Z}{q}\binom{N-Z}{Q-q}}{\binom{N}{Q}}$$

For demonstration purpose, we take a simple example where total number of SNs is $N=170$, with $Z=10$ SNs in each group (i.e., $Y=17$ groups). Fig.3a shows the expected number of compromised groups against the entire network's compromised ordinary SNs.



(a) (b)

Fig. 3. Analytical performance. (a) $E[G_q]$ and (b) $E[X]$.

When 20 SNs are captured, 5 groups having 0 SNs compromised and only 1 group having 3 SNs compromised. Fig.3b demonstrates the number of fully compromised groups that depends on the value z. Four cases are shown when z is 4, 5, 6 and 7. When z is 4, 3(16.66% of entire network) groups are fully compromised against 40 (23.5%) ordinary compromised SNs. But, as the value z increases (6 or 7), number of fully compromised groups are much smaller. We observe that robustness can be improved significantly by increasing the value of z.

5 Related Works and Comparison

Extensive effort has been put so far on how to set up a pairwise shared secret between two sensors and how pre-deployment of secrets is performed to securely communicate among sensor nodes. In Table 3, we briefly compare the prior works and cite major features used including our proposed scheme.

Intuitively, WCDS will, in general, be smaller than connected dominating sets and the resulting induced graph will have smaller edges. This corresponds to fewer clusters and a sparser abstracted network. For comparison, Statistical En-Route Filtering [5] scheme, each intermediate forwarding node verifies one MAC and five hash computations (for Bloom filters) probabilistically if it has one of the keys in common, while in our scheme, only the GDs forward the aggregated report, but they don't perform this intermediate checking. SEF is constrained by sensor's storage

since to increase one hop detection probability, the number of keys a sensor stores should be large. But in our scheme (SMP) only *3* keys are required.

Table 3. Comparison of various security schemes

Schemes	Attacks Defended	Network Architecture	Key Management Scheme	Major Features
Statistical En-Route Filtering [5]	Information Spoofing	Large number of sensors, highly dense wireless sensor network	Partition global key pool and randomly assign m keys from one of the partitions	Detects and drops false reports during forwarding process
Radio Resource Testing, Random Key Pre-distribution etc. [6]	Sybil Attack	Traditional wireless sensor network	Random key pre-distribution	Random key pre-distribution, Registration procedure, Position verification and Code attestation for detecting sybil entity
TIK [7]	Wormhole Attack, Information or Data Spoofing	Traditional wireless sensor network	Used master key to generate other keys. Used Hash tree to generate HMAC for authentication	Requires accurate time synchronization between all communicating parties, implements geographical and temporal leashes
Random Key Pre-distribution [8][9][10]	Data and information spoofing, Attacks in information in Transit	Traditional wireless sensor network	Random key pre-distribution	Resilience, Protect the network even if part of the network is compromised, Provide authentication measures for sensor nodes
REWARD [11]	Black hole attacks	Traditional wireless sensor network	No cryptographic keys, identify malicious node and suspicious area by broadcast messages	Geographic routing, Takes advantage of the broadcast inter-radio behavior to watch neighbor transmissions and detect black hole attacks
SNEP & μTESLA [12]	Data and Information Spoofing, Message Replay Attacks	Traditional wireless sensor network	Each node is given a master key and all other keys are derived from this key	Semantic security, Data authentication, Replay protection, Weak freshness, Low communication overhead
Our Scheme	Insecure bootstrapping, False data injection, Node compromise, Hello Flood attack	Distributed Sensor Network	Star Key Graph based WCDS	Secure SWCDS network formation, Authenticated message delivery, Robustness against node compromise

SEF performs better when the number of hops a packet travels is very high, but SMP scheme has much smaller hops (SWCDS) and the overhead on forwarding aggregated reports gets to the powerful GDs only. Each report is about *15* bytes long in SEF scheme and communication overhead is (*15.h*) bytes, where the number of hops h a report travels is very high (necessary for better performance).

6 Conclusions

In this paper, we have put an effort to devise a security mechanism that combines the star key graph to form a WCDS based distributed wireless sensor network to counteract the impact of compromised nodes. We have shown that star based key pre-assignment has significantly less storage overhead for the individual constrained sensor node and the scheme is also scalable and efficient in storage, communication and computation. We evaluate our scheme through analysis to show that our SMP mechanism is resilient to an increasing number of compromised nodes. For further investigation, some important research issues are worth mentioning: a) To present

experimental results on how often we have to use solutions described in Case I and/or Case II, b) how many messages have to be sent to the BS in order to fix the roles of the nodes after deployment, and c) to validate the analytical results through simulation.

References

1. Garey, M. L. and Johnson, D. S., “Computers and Intractability: A Guide to the Theory of NP-Completeness”, W. H. Freeman, San Francisco, 1979.
2. 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.
3. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless sensor networks: a survey”, Computer Networks 38 (2002), Elsevier Science B.V., pp.393–422.
4. Erdos and Renyi, “On Random Graphs”, Publ. Math. Debrecen, Volume 6 (1959), pp. 290-297
5. 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.
6. 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.
7. Hu, Y.-C., Perrig, A., and Johnson, D.B., “Packet leashes: a defense against wormhole attacks in wireless networks”, Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOM 2003, Vol. 3, 30 March-3 April 2003, pp. 1976 – 1986.
8. Du, W., Deng, J., Han, Y. S., and Varshney, P. K., “A pairwise key pre-distribution scheme for wireless sensor networks”, Proc. of the 10th ACM conference on Computer and communications security, 2003, pp. 42-51.
9. Oniz, C. C, Tasci, S. E, Savas, E., Ercetin, O., and Levi, A, “SeFER: Secure, Flexible and Efficient Routing Protocol for Distributed Sensor Networks”, from http://people.sabanciuniv.edu/~levi/SeFER_EWSN.pdf
10. Chan, H, Perrig, A., and Song, D., "Random key predistribution schemes for sensor networks", In IEEE Symposium on Security and Privacy, Berkeley, California, May 11-14 2003, pp. 197–213.
11. Karakehayov, Z., "Using REWARD to detect team black-hole attacks in wireless sensor networks", in Workshop on Real-World Wireless Sensor Networks (REALWSN'05), 20-21 June, 2005, Stockholm, Sweden.
12. 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.
13. A. Menezes, P. Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, 1996.
14. Y.P. Chen and A. L. Liestman, “A Zonal Algorithm for Clustering Ad Hoc Networks”, International Journal of Foundations of Computer Science. 14(2):305-322, April 2003.
15. Donggang Liu, Peng Ning, and Wenliang Du., “Group-Based Key Pre-Distribution in Wireless Sensor Networks”. In Proc. ACM WiSE’05, September 2, 2005.
16. J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, Wireless Sensor Network Security: A Survey, 2006 Auerbach Publications, CRC Press.
17. C.K. Wong, M.Gouda, and S.S.Lam., “ Secure Group Communications using Key Graphs”, IEEE/ACM Transactions on Networking, vol. 8, no. 1, February 2000.