Asian Journal of Information Technology 12 (9): 297-304, 2013
ISSN: 1682-3915

A Novel Distributed and Secured IRED Protocol for Detecting Node Replication Attack in Wireless Sensor Network

[1]P. Uma Maheswari and [2]P. Ganesh Kumar
[1]Department of MCA, Anna University Regional Centre, Madurai, India
[2]Department of ECE, KLN College of Engineering, Sivagangai (DT), Tamil Nadu, India

Abstract: Nodes of Wireless Sensor Network (WSN) are often deployed in the antagonistic environment and many nodes are unattended. Due to this nature, nodes are easily tracked by the adversary to initiate clone attack. The clone attack is taken through obtaining the credentials of a node in the WSN. They capture and compromise the node and make replicas of them to launch various attacks through the replicated nodes. The cloned nodes are referred as the clones. The clone attack acts as the basic method to mount a huge insider attack. Therefore, it becomes necessary to detect the cloned nodes that are introduced by the adversary in a sensor network. Many techniques and protocols have been proposed to identify the replicated nodes that are presented in the literature review section. Nevertheless they do not meet the requirements in detecting the attack. To address this issue, researchers of this study have proposed a protocol named Intensified Randomized Efficient Distributed (IRED). The proposed research is carried out in two folds. First, researchers have analyzed the properties of the mechanism for detecting cloned nodes. Second, the researchers have proposed the IRED protocol. The proposed protocol is the enhancement of RED protocol. Here, researchers have focused on preventing the clone attack to pervade. Though the protocol prevents the attack, some attack penetrates into the network. In that scenario, the replicated nodes are detected by IRED. The empirical results show that the proposed protocol IRED has higher resistance against the attack and also performs better in terms of computation, memory and communication.

Key words: WSN security, node replication, clone detection, efficiency, distributed protocol, secure IRED

INTRODUCTION

Advancements in technology lead a way to design and develop sensor nodes at very low cost along with off the shelf hardware. These types of sensor nodes are very convenient to deploy a WSN that is of self-organized and distributed network containing numerous numbers of nodes. These are deployed to carry out various monitoring tasks like pollution levels, structural integrity of buildings, freeway traffic, climatic sensing, home environmental sensing, control in office building, light, motion and moisture monitoring and so on. There exits significant challenges in the security of WSN. Threat to the WSN can be of two types (Douceur, 2002): application independent and (Eschenauer and Gligor, 2002) application dependent. The attacks in the application independent category has influence on broad variety of applications from tracking of objects to battlefield surveillance whereas possible attacks found in the latter category is routing, node localization, data aggregation, time synchronization, etc. As the WSN are often deployed in harsh and unattended environment there exist many ways for the adversary to capture and compromise the senor nodes. The compromised nodes are then used to interrupt network operations, insert counterfeit data into the WSN and snoop on the network communication. In such a scenario, clone attacks are launched by the attacker into the network in which the attack captures and obtains the keying materials that are secret from a compromised node and stimulate the generation of replicated nodes that share the keying material and other details of the compromised nodes. Through which the nodes of the WSN are replicated in huge quality and spread it throughout the sensor network. On compromising a single node an adversary can replicate nodes in the network. This type of replication attacks are referred as clone attack. Clone attack is an application independent attack. This attack can be classified through two ways:

- A replicated node is considered completely truthful by its neighbors. In fact, the nodes that are honest are not aware of the clone nodes among them without any global countermeasures

Corresponding Author: P. Uma Maheswari, Department of MCA, Anna University Regional Centre, Madurai, India

- In order to huge number of compromised node an adversaries are not required to compromise large number of nodes. It is more enough to capture and compromise a single node, the cost of compromising the attack has been persistent. Further generation of clones in the network requires and considered very cheap

It is not trivial to detect the clone attack. The major problem in this type of attack is that the replicas possess all information about the security of the compromised original sensor node. Replicated nodes can pass all the identity check thereby escape from being distinguished from a genuine sensor. Moreover, a smart clone tries to hide itself from being identified by all ways. The replicated nodes cheat the administrator of the network into believing that they are authorized. It is evident that the attacker may distribute the replicated nodes anywhere in the WSN. Therefore, this made the localized and centralized detection scheme do not scale well. In addition to that centralized protocols have the disadvantage of high communication cost and single point failure. Essentially, detection of clone nodes in the sensor network is relatively unnoticed research area. The cost of detection is usually computed in terms of storage and communication overhead caused by the detection mechanism in the network.

In this research, researchers focus on both prevention and detection techniques name IRED for clone attacks. Before the construction of the IRED protocol, necessary requirement for and desirable properties of the distributed detection protocol is analyzed. The prevention research is carried in the network is as follows. The detection mechanism usually uses the location information of the nodes to detect a cloned node in a static WSN. But in this study, researchers proposed a technique to detect the clone before it is introduced in to the sensor network. It is achieved through allowing communication among the node nodes continuously and thereby avoids blocking states among the nodes due to the replicated node attack thereby prevents the adversary to penetrate into the WSN. Due to unavoidable reasons the prevention method drop their power against the clone attack in such case researchers used the detection mechanism where the legitimate nodes autonomously detect the existence of replicated nodes and prohibit them from any further network activity. The proposed technique is designed in such a way that its iterations are continuous without effectively affecting the performance of the network; also its detection rate is higher. Moreover, extensive simulations are carried out to prove the efficiency and performance measure of detection mechanism.

LITERATURE SURVEY

This study deals with the reviews related to the issues of clone detection. Initially, centralized solution was proposed by Eschenauer and Gligor (2002) in that the nodes of WSN collect the details of each node location and their neighbor and send it to the base station. If any two nodes in the list contain the same ID with different location then base station concludes that clone attack has been penetrated into the network. However, this technique has the following drawback:

- Single point failure
- As the number of messages required for communication with base station was high it implicitly increased the cost of communication
- Operational life time of the nodes that where nearer to the base station was shorted. Since, those nodes required forwarding enormous number of packets that were from various nodes to base station

Chan *et al.* (2003), Douceur (2002), Eschenauer and Gligor (2002) and Newsome *et al.* (2004) have used location detection as a solution to the clone attack detection. Within the neighborhood nodes they have used the voting mechanism to concur the authenticity of a given node. This technique suffers and fails to detect the cloned nodes that were not within the same neighborhood. Parno *et al.* (2005) have proposed a naive distribution to detect the clone attack in the network. Here, clone attack was detected from the message packets that were flood into the network. Those packets contain the information about the location with that of its neighbor. If a node X's neighbor named Y receives a claim that describes the location of the node Z that was found similar to X but the position was not coherent with X. This scenario leads to the detection of clone attack. Though the technique proposed by Parno *et al.* (2005) performed well in detecting the clone attack it consumed much energy for detection. Since, WSN were energy constrained this technique do not suited well for clone detection. Similar to clone attack, sybil attack by Douceur (2002) and Newsome *et al.* (2004) also, based on the identity. However, both the attacks were independent. A mechanism depending on RSSI was proposed by Demirbas and Song (2006) to address the Sybil attack. Other mechanism such as by Chan *et al.* (2003), Conti *et al.* (2006a, b, 2007a, b) and Di Pietro *et al.* (2006 a, b) have used authentication. They have used the fixed key knowledge for authentication. Node compromise problem was also focused by Conti *et al.* (2006a, b, 2008, 2009a, b), Di Pietro and Mancini (2008) and Zhang *et al.*

(2008). These node compromise detection technique was taken from intrusion detection system (Bonaci *et al.* 2013) seems to need more overhead when compared to done detection techniques. Some secure current solutions were proposed by Conti *et al.* (2009a, b), Di Pietro *et al.* (2009, 2008) and Ho *et al.* (2009) to recover the nodes that were secrecy after node compromising. However, these techniques were not coping with the clone attack. As the centralized mechanism were also not up to the requirement level. Parno *et al.* (2005) have introduced the distributed cloned node detection that was not based on naive distribution. Though this technique scales good, it does not meet the emerging requirements. To fulfill those requirements (Gligor, 2006) have introduced two distributed detection protocol. The two protocols were named as follows:

- Randomized Multicast (RM)
- Line-Selected Multicast (LSM)

The first protocol selects a group of random nodes to distribute the location of all the nodes in the network. Whereas LSM used the routing topology of the sensor network in order to find the replicated node. When a node broadcast locally its location every node that were neighbor to that node signs a copy of its claim containing information about location to a set of selected node. This technique always used random selection. This mechanism requires high communication cost. To overcome this problem LSM was proposed. It used the routing topology of a sensor network to find the replicated nodes. LSM was enhanced by Zhu *et al.* (2007) to increase the probability of detection given by LSM. In Song *et al.* (2007), an interesting distributed detection protocol termed SET was proposed for node replication attack. Random values generated by BS was influenced by SET to carry out the detection these values were used to produce cluster heads and cluster. This protocol used generates the cluster iteratively. If an ID of a node present in two different independent clusters then it was decided that the node having the corresponding ID was cloned. The major problem with this protocol was that an adversary can exploit the protocol with the aim to revoke the nodes that were not cloned. Due to this reason most of the research scholars have not used SET as their bench mark technique. Requirements for the detection protocol have been discussed in the study of Conti *et al.* (2006a, b). According to it, LSM fails to satisfy the mentioned requirements. It suffers from some problems that were as listed:

- There exists a higher probability for some nodes in the WSN to act as witness
- Also, there exist highest possibilities for an attacker to compromise the witness nodes
- Communication overhead was not evenly distributed among the nodes of the sensor network

To overcome these disadvantages, Conti *et al.* (2007a, b) have proposed a new protocol named Randomized, Efficient and Distributed (RED) protocol which also satisfies the requirements of Conti *et al.* (2006a). RED was a self healing mechanism and also it denotes that their performance was better than LSM mechanism in terms of communication, detection, memory and computation.

Bonaci *et al.* (2013) have studied the communication and storage cost the existing replicated node detection algorithms and protocols. In addition, to their study they have proposed an optimized approach for distributed detection of cloned nodes. They have investigated on the witness-based detection mechanism. Bonaci *et al.* (2013) have developed an optimized framework for electing the parameters of the detection mechanism which reduced the clone attack. They have also showed that the detection method can be described in terms of the following cost:

- Influence of leaving the undetected replicated nodes in the sensor network
- The cost in detecting a non-compromised node as compromised node
- Storage and communication cost

All the techniques that were proposed earlier has an assumption that the nodes deployed in WSN has very less or no mobility (i.e., static nodes). To address the clone attack issue in mobile sensor network, Bonaci *et al.* (2011) have used Sequential Probability Ratio Test (SPRT). This technique simulates the neighbor of a node that has moved to new location to ask for the claim to measure the probability and decide whether to forward or to drop the claim to base station. SPRT focused the basic idea of mobility of a node that a node do not exceeds the speed of the system configured speed.

THREAT MODEL

Certain amount of nodes is deployed in the network and they pass their information to the sink node that gathers and then forward it to the access point. These access points are responsible to have further communication with the base station and the destination node correspondingly. Researchers defined simple yet powerful adversary threat model. The defined attackers are possible to compromise a certain fixed amount of

nodes and replicate one or multiple clones into the network. In order to handle with the threat, it would be probable to assume that nodes are tamper-proof. Researchers have also assumed that the nodes are stationary and the adversary would be in and around the network environment such that they can gain the access of access point nearer to BS and launch clone attack. Then, the adversary can compromise single or few nodes through obtaining the cryptographic information of the compromised node by which it produce the clone and insert it into the network. The compromised as well as cloned nodes are fully controlled by the adversary and can communicate with each other at any time. By this way, the attacker changes the data that are required and send it to the access point. Therefore, access-points are made more intelligent to avoid the penetration of an adversary. In case if the adversaries are more powerful then the preventing method of IRED drops its power, from where the detecting mechanism starts. The detection mechanism has the assumption that the goal of the adversary is to weaken the detection protocol that is distributed by compromising a minimal subset X of the nodes. The adversary has compromised Y nodes (a set of nodes) already while TN is the total number of nodes in the sensor network. For every node z, the node request $P_w(z)$ returns the probability that $z \in TN \setminus Y$ is a witness for next run of the protocol.

INTENSIFIED RANDOMIZED EFFICIENT DISTRIBUTED PROTOCOL

Requirement for IRED protocol: The following are the major requirements that should be meet out by the distributed detection mechanism:

- Overhead
- Witness distribution

Overhead: Due to the resource constraints of the sensor network, it is often very difficult to design protocol for detection of such attack. Therefore, it is mandatory to produce little overhead on the network. In addition to the above requirement, it also required to distribute the overhead to the entire network. Since, during the execution there may be possible for a subset of entire node to experience much higher overhead. If such situation arises then the nodes present in the subset exhaust their energy quickly as a result those nodes fails to carry out network operation. Further this is more suitable when memory is considered. If memory overhead is higher for a subset of nodes in the network then it may be possible for these nodes to overflow. During overflow, it is not possible for the node to execute the protocol. These requirements implicitly express that the overhead produced by the detecting protocol should be small and distributed evenly among the nodes.

Witness distribution: Choosing witnesses for detecting the clone attack is the major issue in WSN. If an attacker is able to detect the future witnesses in prior to the detection protocol execution then it is easier for the adversary to interrupt the network so that the attack is not identified. Two different kinds of witness predictions are given.

Location-based prediction: The probability for a witness of a node does not depend on the geographical location of the corresponding node.

ID-based prediction: The protocol does not provide any information about the ID of a node in the network which may be the witness for the protocol for next run.

IRED protocol

Before pervading (prevention): The attackers can be blocked if the access-point is more intelligent that it is capable to block the communication or accepting the data from original and cloned nodes. The assumptions made on access-point is that it receives or accepts the data packets from original and malicious nodes at different time of interval. The details of those data packets are recorded in data base. The variation in the recorded details makes confusion to the readers. If the access-point is able to block the communication nodes with same ID then it can remove conflict ID and data from the node and also, announces all the nodes about the occurrence of replication.

In order to obtain access to access-point an attacker usually tries to insert the cloned node through the intermediate nodes of the network through a multi-hop communication. In such a scenario if there is no proper updates for the nodes in the network. Then, they are not able to have clear idea of the new node entry. In this situation, researchers distribute the IRED protocol of prevention method among nodes that validate and prevent the new entry of nodes based on few constrains. Therefore, the cloned node are removed at the access-point itself without affecting the communication among original legitimate nodes.

After penetration (detection): In case if the adversaries are more powerful then the preventing method of IRED drops its power from where the detecting mechanism starts. Two steps are involved in detection of clone

attack. At the first step, among the nodes of the network, a random value is shared. This value is then broadcasted with a centralized mechanism. Once the random value is shared successfully among the nodes then the second step on detection of the clone node is determined.

In the second step each node signs digitally and broadcast the geographic location and the claim ID. On receiving the broadcast message, they claim a subset of network locations that are selected pseudo randomly. If a claim is sent to a node's ID that is no longer alive in the network then such claims are lost. First deployed nodes are alone considered for witness. The IRED can easily adapted to work when a particular node is used as the message destination. For the detection purpose, the researchers have assumed that the messages of a node are sent to another node that is very closer to the sender nodes location. In addition to that, it is also assumed that the protocol never fails and forwarding message is not affected by wormhole attack or by dropping. Moreover, adversaries are capable to manipulate the witness set. However, it consumes more time to compromise those nodes because reaching them the detection protocol efficiently determines and avoid it.

EXPERIMENTAL RESULTS

In this study, researchers have compared the IRED with RED and showed that IRED performs much better than the RED algorithm in several ways. The experiment is carried out using the Software NS2 Version 2.35. The simulation is taken with 800 nodes in WSN and communication radius as 0.2. The nodes are uniformly distributed in the network at random manner. The performance of the IRED is computed for the storage, detection accuracy, packet delivery ratio and true positive.

Storage overhead: The major issue that gains more attention for the detection mechanism is the storage. The detection protocol requires certain amount of memory of all the nodes in order to execute in the corresponding network. It is more important that the detection protocol should get utilize less memory to get executed in the nodes since sensor nodes are normally resource constraints. Figure 1 explains the storage overhead caused by the IRED and RED detection protocol. It stands evident for the IRED that it needs very less memory and causes very low overhead on the sensor nodes. Therefore, IRED outperforms RED in terms of storage requirements.

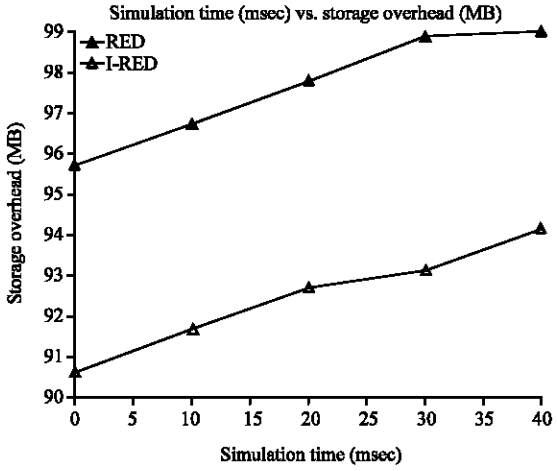

Fig. 1: Storage overhead

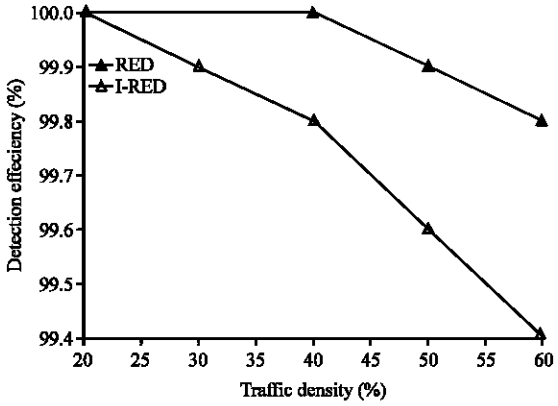

Fig. 2: Traffic density vs. detection efficiency

Detection efficiency: Efficiency of a protocol in detecting the clone attack depends on the density of the traffic and number of nodes in the sensor network. Figure 2 expresses efficiency of the proposed algorithm in determining the clone attack at various traffic density. It also expresses that the detection efficiency for the IRED protocol is higher than the RED protocol. Initially while the traffic is lesser, i.e., <20% the detection rate of the RED and IRED are the same. Whereas when the traffic increases >20% then the performance of the RED protocol decreases gradually. In case of IRED, the detection efficiency is constant up to the 40% and start decreases only after the traffic density increases >40%.

Detection efficiency is also, affected by the number of nodes in the network. Figure 3 represents the detection capacity of the protocols for different number of nodes in the network. It is evident that the RED protocol performs better only when there is large number of nodes whereas it detection efficiency is normal when the number of

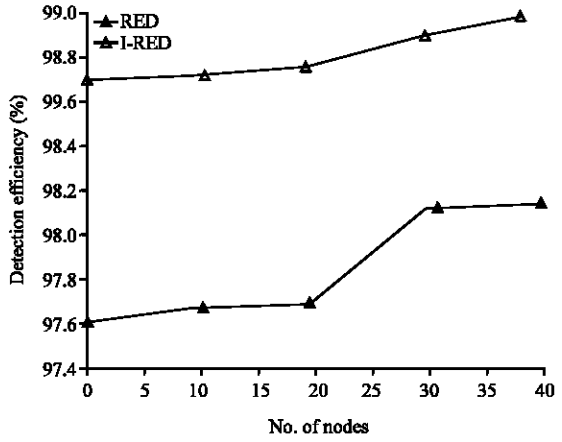

Fig. 3: Number of nodes vs. detection efficiency

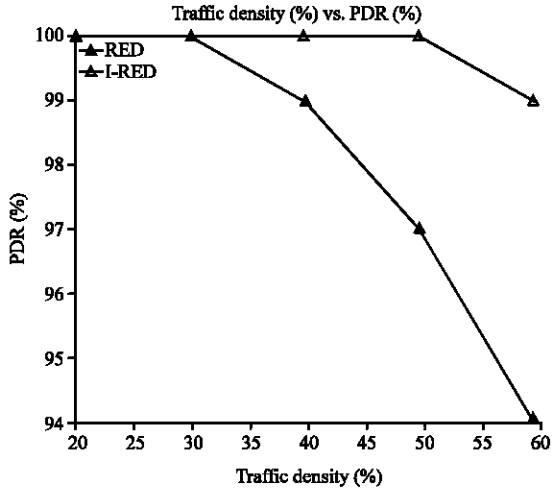

Fig. 4: Packet delivery ratio

nodes are lesser. For the IRED protocol the detection efficiency increases the number of node increases continuously.

Packet delivery ratio: Delivery ratio is the more important factor in WSN. As the sensor nodes are normally deployed with very less storage capacity it may drop the packets when they are overloaded. So, the design of the detection protocol should not overload the nodes. If the nodes are overloaded then the packet delivery ratio gets decreased. Figure 4 portrays the packet delivery ratio of the nodes in the network while executing the detection algorithm. It also, shows that the number of packets delivered to the sink node is higher for the IRED protocol even when the traffic increases while comparing with the RED protocol. It explicitly denotes that the IRED protocol has less computation overhead than the RED protocol. Therefore, it can be implemented effectively in the sensor networks.

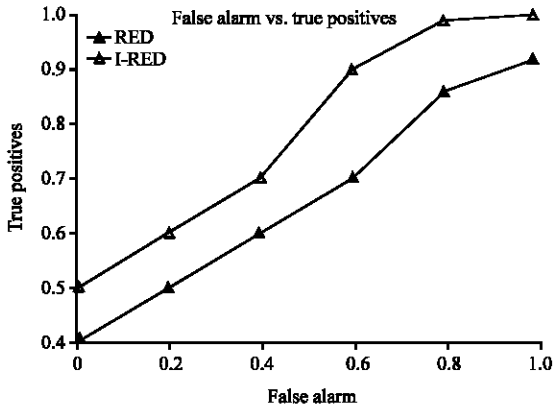

Fig. 5: True positive

True positive: It is essential to find the attack correctly, i.e., the normal operations should not be detected as the clone attack. This measure is computed in the Fig. 5. It represents that the IRED detect the clone attacks more correctly than the RED protocol.

CONCLUSION

The most daunting problem in sensor network is the clone attack. This attack acts as the basic step to launch a huge insider attack. Various methods are proposed to detect the existence of the clone attack in the network. But those techniques are not satisfying the desirable properties of the detection techniques. In order to detect the clone attack as well as satisfying the detection algorithm techniques researchers proposed the IRED protocol. Before designing the protocol for detection, researchers have studied the requirements of the detection etiquette.

This protocol initially prevents the attack to exist into the network this technique. Prevention technique present in the access-point of the network to monitor the penetration of attack. Though the detection algorithm effectively blocks the attack earlier some effective adversary may break the prevention technique and pervade into the network. Such pervaded attacks are detected using the detection technique. They determine the existence of the attack from the witness. The efficiency of the proposed IRED protocol is experimented in terms of storage overhead and the detection capacity in the network.

As the IRED protocol is capable of being implemented in a network having very less or no mobility areas out future research concentrates in enhancing the IRED protocol to detect the clone attack in the mobile network.

REFERENCES

Bonaci, T., P. Lee, L. Bushnell and R. Poovendran, 2011. Distributed clone detection in wireless sensor networks: An optimization approach. Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, June 20-24, 2011, Lucca, Italy, pp: 1-6.

Bonaci, T., P. Lee, L. Bushnell and R. Poovendran, 2013. A convex optimization approach for clone detection in wireless sensor networks. Pervasive Mobile Comput., 9: 528-545.

Chan, H., A. Perrig and D. Song, 2003. Random key predistribution schemes for sensor networks. Proceedings of the IEEE Symposium on Security and Privacy, May 11-14, 2003, Berkeley, CA., USA., pp: 197-213.

Conti, M., R. Di Pietro and L.V. Mancini, 2006a. Secure cooperative channel establishment in wireless sensor networks. Proceedings of the 4th Annual International Conference on Pervasive Computing and Communications, March 13-17, 2006, Pisa, Italy, pp: 327-331.

Conti, M., R. Di Pietro, L.V. Mancini and A. Mei, 2006b. Requirements and open issues in distributed detection of node identity replicas in WSN. Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, October 8-11, 2006, Taipei, Taiwan, pp: 1468-1473.

Conti, M., R. Di Pietro and L.V. Mancini, 2007a. ECCE: Enhanced cooperative channel establishment for secure pair-wise communication in wireless sensor networks. Ad Hoc Networks, 5: 49-62.

Conti, M., R. Di Pietro, L.V. Mancini and A. Mei, 2007b. Efficient and distributed protocol for the detection of node replication attacks in wireless sensor networks. Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing, September 9-14, 2007, Montreal, Quebec, Canada, pp: 80-89.

Conti, M., R. Di Pietro, A. Gabrielli, L.V. Mancini and A. Mei, 2009a. The quest for mobility models to analyse security in mobile ad hoc networks. Proceedings of the 7th International Conference on Wired/Wireless Internet Communications, May 27-29, 2009, Enscheda, The Netherlands, pp: 85-96.

Conti, M., R. Di Pietro, L.V. Mancini and A. Mei, 2009b. Mobility and cooperation to thwart node capture attacks in MANETs. J. Wireless Commun. Network., 10.1155/2009/945943.

Conti, M., R.D. Pietro, L.V. Mancini and A. Mei, 2008. Emergent properties: Detection of the node-capture attack in mobile wireless sensor networks. Proceedings of the 1st ACM Conference on Wireless Network Security, March 31-April 2, 2008, Alexandria, VA., USA., pp: 214-219.

Demirbas, M. and Y. Song, 2006. An RSSI-based scheme for sybil attack detection in wireless sensor networks. Proceedings of the International Symposium on World of Wireless, Mobile and Multimedia Networks, June 26-29, 2006, New York, pp: 564-570.

Di Pietro, R. and L.V. Mancini, 2008. Intrusion Detection Systems: Advances in Information Security. Springer, London, UK., ISBN-13: 9780387772653, Pages: 264.

Di Pietro, R., D. Ma, C. Soriente and G. Tsudik, 2008. POSH: Proactive co-operative self-healing in unattended wireless sensor networks. Proceedings of the IEEE Symposium on Reliable Distributed Systems, October 6-8, 2008, Naples, Italy, pp: 185-194.

Di Pietro, R., L.V. Mancini, A. Mei, A. Panconesi and J. Radhakrishnan, 2006a. Sensor networks that are provably resilient. Proceedings on the International Conference on Security and Privacy in Communication Networks and the Workshops, Auguest 28-September 1, 2006, Baltimore, pp: 1-10.

Di Pietro, R., L.V. Mancini and A. Mei, 2006b. Energy efficient node-to-node authentication and communication confidentiality in wireless sensor networks. Wireless Networks, 12: 709-721.

Di Pietro, R., L.V. Mancini, C. Soriente, A. Spognardi and G. Tsudik, 2009. Playing hide-and-seek with a focused mobile adversary in unattended wireless sensor networks. Ad Hoc Networks, 7: 1463-1475.

Douceur, J.R., 2002. The Sybil attack. Proceedings of the 1st International Workshop on Peer-to-Peer Systems, March 7-8, 2002, Cambridge, MA., USA., pp: 251-260.

Eschenauer, L. and V. D. Gligor, 2002. A key-management scheme for distributed sensor networks. Proceedings of the ACM Conference on Computer and Communications Security, November 18-22, 2002, Washington, DC., USA., pp: 41-47.

Gligor, V.D., 2006. Emergent properties in ad-hoc networks: A security perspective. Proceedings of the Symposium on Information, Computer and Communications Security, October 30-November 3, 2006, Alexandria, Virginia, pp: 1.

Ho, J.W., M. Wright and S. Das, 2009. Fast detection of replica node attacks in mobile sensor networks using sequential analysis. Proceedings of the 28th IEEE International Conference on Computer Communications, April 19-25 2009, Rio de Janeiro, Brazil, pp: 1773-1781.

Newsome, J., E. Shi, D. Song and A. Perrig, 2004. The sybil attack in sensor networks: Analysis and defenses. Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, April 26-27, 2004, Berkeley, CA, USA., pp: 259-268.

Parno, B., A. Perrig and V. Gligor, 2005. Distributed detection of node replication attacks in sensor networks. Proceedings of the IEEE Symposium on Security and Privacy, May 8-11, 2005, Oakland, CA., USA., pp: 49-63.

Song, H., L. Xie, S. Zhu and G. Cao, 2007. Sensor node compromise detection: The location perspective. Proceedings of the International Conference on Wireless Communications and Mobile Computing, August 12-16, 2007, Honolulu, HI., USA., pp: 242-247.

Zhang, Q., T. Yu and P. Ning, 2008. A framework for identifying compromised nodes in wireless sensor networks. ACM Trans. Inform. Syst. Secur., Vol. 11 10.1145/1341731.1341733.

Zhu, B., V.G.K. Addada, S. Setia, S. Jajodia and S. Roy, 2007. Efficient distributed detection of node replication attacks in sensor networks. Proceedings of the 23rd Annual Computer Security Applications Conference, December 10-14, 2007, Miami Beach, FL., USA., pp: 257-267.