ISSN 2250-3153

Classification and Aanalysis of clone attack detection procedures in mobile wireless sensor networks

M.H Ansari*, V. TabatabaVakily*

* Department of Communication Engineering, Iran University of Science and Technology (IUST), Narmak IUST, Tehran, Iran

***Abstract*-** In this paper, regarding accelerating development of mobile sensor nodes technology and increasing the utilization of them and alsothese networks are faced with security challenges; specially clone nodes attack, our focus is on exploiting optimum criteria of node clone intrusion detection procedures in mobile wireless sensor networks by using theoretical analysis of procedures. Since many of recommended protocols in this area have not been experimentalised and also no comprehensive study has been carried out on the possibility and capability of these procedures, in this paper all types of sensor network architecture, with the presence of mobile sensor node, are analyzed and then according to the type of architecture, the procedures of clone node intrusion detection is classified and meticulously scrutinized. Finally the conclusion is presented based on theoretical analysis.

***Index Terms*-** wireless sensor network (WSN), clone attack, intrusion detection, mobility.

I. Introduction

Utilizing WSNs in different environments, such as medical and military areas, because of the inexpensiveness, self-organizing and not needing constant supervision of sensor nodes is increasing. But regarding the inexpensiveness of sensor nodes, lack of physical shield layer on these nodes and utilizing them in enemy environment without protection, usually these networks are at the exposure of different internal and external attacks [1-4]. Because of the limited energy and memory sources of these sensor nodes, the security challenges in these networks are encountering more complexity as compared to other mobile telecommunication networks. These complexities are intensified if the sensor nodes have mobility. Regarding the structure and architecture of WSNs among different attacks introduced in papers [1-7], because of the clone node attacks capability in passing through encrypting layer and authentication and also proper conditions for other attacks, these attacks are considered as the most serious security threats for the WSNs. In clone node attacks, first the attacker compromises the network sensor node and then by using side channel attacking techniques exploits the information on the node in a certain amount of time and finally uploads the information on any number of nodes. Now the attacker can make any type of attack on the network by taking the control of these nodes. Because after compromising the node, the attacker exploits the confidential information, including secret keys and uploads it on other clone nodes. From point of view of other nodes, the clone nodes seem to be valid. To avoid these types of attacks, new defensive solutions are required as a second security layer. Regarding the importance of this subject, many researchers have focused their efforts on it and a lot of procedures have been recommended for this attack. By analyzing various procedures, it can be observed that different criteria and variant methods and sometimes impractical hypotheses are considered, in which, simulation by real conditions such as the life of the battery, lower layer protocol, and real mobility models can clearly prove this point. Furthermore, choosing criteria, hypotheses, and as the result, proper detection procedure in the networks is essential.

What we know so far, no precise and experimental investigation has been implemented on WSNs with mobile nodes, so because of the requirements and vast domain of architectures and WSNs configuration, in this paper, it has been concentrated on this type of network. In section II, based on the presence of the mobile wireless sensor node, all types of configurations are assessed, then according to the type of wireless sensor nodes (static and mobile) a new classification is suggested and the hypotheses and the capabilities of the attacker and the network in each configuration are described. In sectionIII, with regarding to effective criteria and parameters, the intrusion detection procedures in mobile WSNs will be mentioned and accurately investigated. In fact, WSNs with mobile node are divided into three groups: static WSN with mobile attacker, static WSN with mobile intrusion detection nodes and mobile wireless sensor network. Then the intrusion strategy is divided by using the criteria of being centralized or distributed, homogeneous or hierarchical, of the network structure. In section Ⅳ, the intrusion detection procedures in WSN with mobile nodes, by taking into consideration the criteria of part III are accurately analyzed, and classification is carried out based on theoretical analysis. At the end, in section Ⅴ, the conclusion of the theoretical analysis is presented.

II. Network and attacker model

1)Network model

The WSN usually contains hundreds and sometimes thousands of cheap and small size wireless sensor nodes, which are accidentally or in a pre-designed way distributed in a vast geographic area. In WSNs it is assumed that every moment there is the possibility that a number of sensor nodes get lost or be added to the network [1]. While in old networks, all the sensor nodes are static and have a base station for gathering data, today, respecting the robotics technology advancement and the emergence of mobile wireless sensor nodes, the structure of sensor networks has been changed. Different types of sensor networks with the combination of mobile and static are illustrated in figure (1).

Therefore, here it is assumed that wireless sensor nodes are mobile and regarding this criterion, the networks are considered based on below architectures;

i. Mobile-WSN (MWSN): in this network all of the nodes have mobile capability.
ii. WSN with mobile attacker: in this network all of the network sensor nodes are static but the attacker has mobile capability.
iii. WSN with mobile intrusion detection node: in this network all of the network sensor nodes are static but the intrusion detector nodes have mobile capability.

Besides, here in hybrid networks it is supposed that mobile nodes have more potential and sources compared to static nodes. Because of the more intensity of security challenges in homogeneous networks, the general architecture of homogeneous networks is considered.

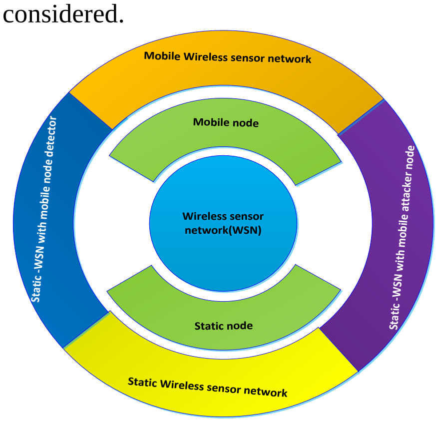

Figure1. Schematic diagram of all types of wireless sensor networks in terms of nodes mobility

2) Attacker model

With referencing to the definition of clone node attack [7-9], in this attack, the attacker compromises between one or some network nodes and exploits their stored information and replicates a preferred number of nodes from a certain node with specific identity and places them in appropriate locations in network, so that respecting the desired goals, it will be able to make different attacks including, eavesdropping, DoS, inject fake data and attacking the network protocols. Also it is assumed that the attacker is not able to allocate a new identity to the clone nodes and mostly the attacker can only compromise a small part of the network nodes. Otherwise, with referencing to clone attacks costs, there is no need for node replicate. In addition, it is assumed that the attacking nodes can communicate and even collude with each other. It is also possible that the attacker nodes have more capability and flexibility compared to the valid nodes of the network which is a reasonable hypothesis. Finally, it is supposed that the attacker nodes can use various mobility models for moving in the network. But, due to the RWM model is comprehensive and ideal, in this paper it is assumed that the attacker utilizes this model. Indeed, from a general point of view, the attacker node can be either mobile or static in the network.

3) Framework for clone node intrusion detection

Regarding to the point that in clone node attack, first the attacker compromises one or some nodes and then exploits the information, second, by reprogramming the information in desired number of nodes, next, places it in appropriate location in order to fulfill the desired goals. Therefore, after the attack is implemented by the attacker, the clone node requires a reciprocal link between itself and the neighbors, then shares the session keys for creating secured link and eavesdrops the information which is sent by neighbors and attacks controlling protocol in the network. But before creating all these communications, all the nodes added to the network are forced to pass through intrusion detection protocol as the second security layer. In other words unless the attacker nodes have not passed the intrusion detection process, they are not able to fulfill their malicious goals. According to this framework, the attacker for being successful and reaching is desired goals should pass the detection protocols designed for the wireless sensor network. Consequently, real and exact analysis of the protocols and intrusion criteria, regarding the limitations of the WSN and simulating them with real protocol layers are essential. Hence, in order to assess the performance procedures with real hypotheses, they are theoretically analyzed and classified.

III. Intrusion Detection Procedures in Wireless Sensor Networks with Mobile Node

Regarding the hypotheses of the network model, in this paper, network configurations, in terms of combination of sensor nodes, are divided into three categories:

i. All the nodes of mobile wireless network
ii. mobile attacker node
iii. Mobile detection node.
iv. Then the suggested procedures, based on the criteria of being centralized or distributed, local detection or involvement of the whole network in detection process, or being based on conflict with more details are divided. Thus, from Fig.2 it can be observed that the intrusion procedures based on detection method, performing strategy and detection criterion, are divided.

1) Clone node detection procedures in mobile wireless sensor network

While all the nodes of WSN have mobility, considering the mentioned criteria in section 2, the clone node detection attack procedures are divided as follow:

A. Locally-distributed detection procedures, based on conflict

According to our knowledge, first time in [12], a distributed clone detection procedure named as XED, has been proposed for MWSNs.

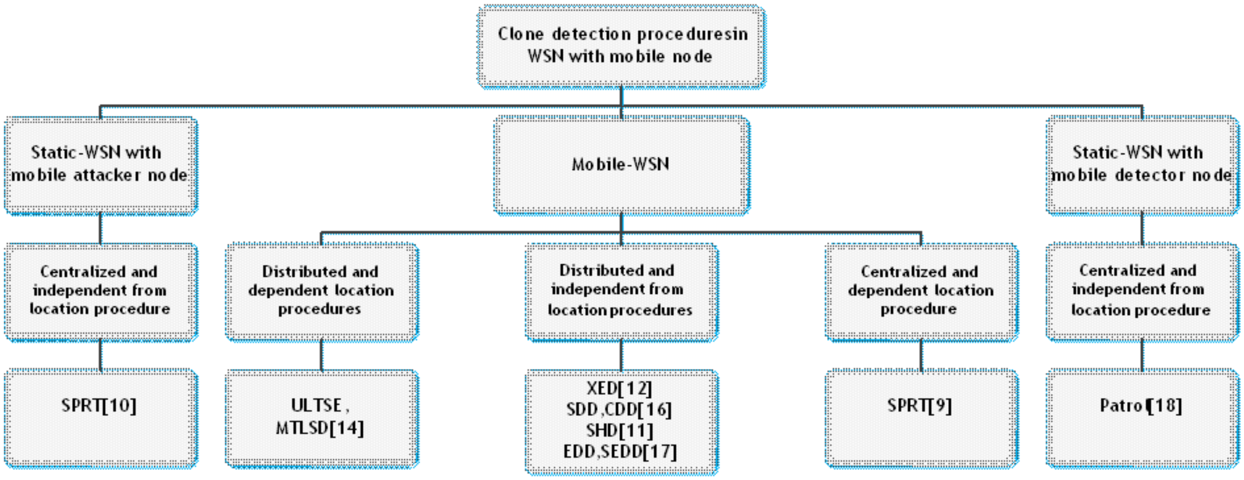

Figure2. Classifications of WSNs detection procedures with mobile node

Regarding to the previous experiences, because of high communication overhead in selecting witness nodes, energy limitations and continuous routing changes in MWSNs, XED ignores the location information criteria for identifying the clone node. Indeed, XED applies "challenge and remember" strategy for detecting the presence of the clone node. In fact, in the accepted strategy in XED, it has been supposed that the sensor node is equipped with a random number generator and has a unique identity. In this protocol when the s_i and s_j arrive at the communication domain of each other, any of them will produce the random numbers of r_{s_i} and r_{s_j} respectively and exchange them, then the received and sent numbers together with identities will be stored in any of the nodes. When s_i and s_j meet each other once again, at first the previous random numbers are exchanged and checked in any node, whether the received and stored numbers are equal or not. In this case if they are not the same, the clone intrusion is detected and node identity revoke message is broadcasted throughout the network. Otherwise the random numbers are exchanged and replaced with the previous ones. It is observed that the algorithm has low memory overhead. But the detection probability is not high. Also, because of the communication and storage error, there is the probability of negative and positive errors. Also, XED is vulnerable to smart attacker and collusion of the nodes.

B. Central clone detection procedure based on the criteria of speed

In [9], due to the fact that the majority of wireless nodes speed are limited, authors has defined speed threshold(V_{max})as detection criteria. Central clone node intrusion detection procedure is proposed based on the location information for the MWSNs. In this paper because of the probability of increasing the positive and negative errors resulted by calculation error in measuring speed or lack of simultaneity among the nodes, SPRT mechanism is used. In fact the authors have proposed their procedures by assuming that the network nodes are aware of their location and RTM mobility model is used. Generally, in this procedure when the mobile sensor nodes reach the desired location, first by using localization protocols, positions are located and their claims $C_i = \langle ID, T_i, l_i, H(ID||T_i||l_i)Sig_i \rangle$ are sent to their neighbors. Secondly the claim message is authenticated and Neighbors with the probability of p send claim to BS. After authentication of the node i message, the base station calculates the speed at the $i+1$moment, by using C_i and C_{i+1}information and compares the results with V_{max}. Then this procedure assumes distribution as Bernoulli random variable and by calculating the logarithmic probability rate for n samples received claim of the node i, carries out the decision making process it. So when SPRT exceeds its higher bound, the clone node will be identified and the revocation message broadcasts in the network.

C. Locally distributed clone node attack detection procedure, based on the time of exploiting the information on the compromised node

To replicate clone nodes from a certain node of the network, we need to separate it from the network and then spend time for exploiting the information. In [16], by using this fact, the SDD procedure has been proposed for intrusion detection in MWSN. In reality the suggested solution in [16] is based on the fact that if node a does not meet node b twice in an λ interval, we can probably conclude that the node b has been separated from the network by the attacker to be replicated. The accuracy of SDD procedure depends on an interval with high probability that nodes may meet each other. Indeed the detection takes place within a trade of detection time and rate of positive error. In SDD each node is considered as a witness for the rest of the network nodes and thus each node should send a message throughout the network for announcing its presence, which increases the communicative overhead and energy consumption. It is also observed that the detection probability of SDD is not high and to improve that, authors in [16] by using participation of the neighbors and exchanging the information of the joint nodes, proposed CDD procedure. New procedure increases the detection probability and decreases the negative error; but increases the communication overhead and memory.

In [17] with an attitude different from [16] and regarding the fact that the number of the meets of two nodes in a certain interval with a high probability is restricted, EDD procedure is proposed. EDD procedure contains two phases; one of them is offline phase and deals with calculation of interval length and threshold of the meets of two nodes in a certain interval, and other one is online phase that deals with exchanging and comparing the messages of different nodes and detects node clone attack. By analyzing EDD, it is observed that this procedure is vulnerable to smart attacker, and also has high memory overhead. In order to solve the second problem, by using an exchange between the memory and the interval length, authors in [17] have proposed SEDD procedure. In SEDD each node analyzes only one set of nodes named monitor set and stores their messages; by doing this the memory of the nodes is saved.

D. Locally-Distributed Detection procedure based on mobility

Authors in [14], for the purpose of the clone node detection in mobile wireless sensor network, proposed UTLTSE procedure based on mobility and awareness of the node location. In this procedure it is assumed that after the witness nodes receive time-location claim, instead of sending them, carry the claim all over the network and exchange the claims when the witness nodes meet each other. In fact the important advantage of this protocol depends on movement of the nodes and independence from downer layer routing protocol. In UTLSE protocol, each node is forced to trace a certain set of the nodes and all the witness nodes store only one location-time claim. So when witness nodes arrive at the radio domain of each other, exchange the claims and carry out the detection protocol. of course it must be noted that in this procedure, the detection process is always done with smaller ID nodes. With precise analysis it is observed that sometimes detection fails, because two witness nodes before they meet each other, they meet a third clone node. In order to solve this problem and increase the probability of detection, authors in [14], proposed MTLSD procedure, which benefits from ULTSE principles and uses of a queue with at least two lengths and the optimum of three lengths.

E. Locally Distributed detection procedure based on the list of the neighbors

In [11], by extending the routing problem with the help of mobility, authors proposed distributed intrusion detection procedure (SHD) for mobile wireless sensor network. Regarding that access to the location information is a strict hypothesis and the mobility models are different, SHD procedure dispenses with these two criteria. So SHD procedure uses the exchanging list of the neighbors among the mobile nodes and selects witness nodes for detection. This procedure is protected against the collusion of the attacker nodes. Generally, the detection process in SHD is based on sending the message of $\langle ID, neighbor - list\rangle$ to the nodes in its communication range at the first time the protocol is performed and then uses question and answer method.

F.Centralized detection procedure based on key pre-distribution

Authors in [13], by using the pair-wise pre-distribution key and bloom filter have proposed a centralized detection procedure, which is independent from the location of wireless sensor nodes. Generally, by assuming that the base station is trusted, the server key method is applied and its confidentiality is always maintained. Then by using a two variable polynomial in $GF(p)$,unique confidentiality pair-wise key is produced and loaded on each node. Also In this procedure, to decrease communication costs, alongside server key method, bloom filter method is used. Then, in order to communicate with the neighboring nodes and by using functions and filters, each node produces a pair-wise key and shares it with the neighbors. In the next phase, each node sends a ciphering report to the BS containing its ID and CBF. After receiving all the reports, BS deciphers them and counts the number of created keys of each node. Regarding that, at first the keys have been distributed uniformly and the mobility model is RWM; statistic of producing keys of legally nodes should be close to each other. Thus, if the number of keys of a node is more than the predetermined threshold, it can be concluded that the replicated node and the message of revoking it from network has been announced by BS.

2) Clone node detection procedure, for static sensor networks with mobile detector node

Regarding the limitation of energy consumption and high amount of communication overhead of detection procedures based on static nodes with progresses made in the technology of micro-robots, authors in [18], proposed a clone node detection procedure by using mobile wireless sensor nodes. In Patrol procedure the network model is considered as a combination of mobile and static nodes. Also it has been supposed that the static nodes have access to their location information. So, regarding the attempt made by the attacker for compromising the static and patrol nodes and the possibility of presence of two mobile and static clone nodes, two criteria are introduced and utilized in the procedure: "each single node only is in one location in any moment" and "maximum speed of mobile node".

The Patrol procedure is based on assumption that for the purpose of providing a secured communication all the static nodes require exchange of confidentiality information among static nodes with the patrol nodes. By moving throughout the network and inspecting the static nodes, Patrol nodes collect their claim. It is supposed that when the static node cannot communicate the patrol in any round, the static node will be separated from the network in the next round. In addition, in [18] it is assumed that each static node is inspected by at least two patrol nodes in the network and any of them is considered as the reference node. In Patrol procedure the static node detection is carried out by receiving the nodes location claims with the patrol node and analyzes the location conflict among the nodes with identical IDs. Under these circumstances, communication cost in comparison with the traditional detection procedures such as LSM [7] and RED [21] decreases greatly. Besides for situations in which the attacker compromises the patrol nodes, the procedure uses the maximum speed criteria in central or distributed method and performs the detection by the static nodes.

3) Clone node detection procedure, for static sensor networks with mobile attacker

Usually for attacking the network protocols like routing and clustering protocols, the attacker requires a large number of compromised nodes. For a lot of attackers it is hard and sometimes impossible to achieve this goal. Due to the above mentioned circumstances, if attacker uses mobile nodes and they become member in the list of different nodes neighbors at the time of preparing the list by the network nodes, the DDoS capability for the attacker is provided [4]. So, since the static detection protocols are not able to detect the DDoS attacks, imposing limitations to the attacker is not a reasonable assumption to confront the attacks made in the network. Therefore in [10], authors proposed a distributed procedure to detect the mobile attacker node and it has been supposed that the network applies the traditional methods like RED and LSM to detect the static attacker. In fact [10] has used an unusual silence criterion of the neighboring node in order to detect the clone node and has established a procedure independent from the location information. Also to increase the precision of detection, SPRT technique has been utilized. Furthermore the detection of the virtual mobile nodes is done by using RSSI technique.

IV. Theoretical Analysis of the Detection Procedures

In this section, we will discuss about the necessity of non-deterministic and full distributed detection procedures and then represent security requirements that should be fulfilled by the detection procedures.

1) Selecting the type of protocol

First, we will discuss the procedures with the highest distribution rate against the procedures having central controlling node. Usually the central controlling node (BS) decreases the complexity of the detection procedures as compared to distributed procedures [7]. But worse problem in centralized procedures is the presence of BS as the error point, which leads to the extreme decrease of the energy of the neighboring nodes compared to the other nodes networks, and also causes security threats in the network.

The next essential scrutiny is the analysis of the deterministic protocols in comparison with non-deterministic procedures. Because of the probability nature of non-deterministic protocols, attacking is difficult for any attacker [49]. In deterministic procedures, at the time of performing the protocol, the witness node protocols are considered unchangeable. Thus, if the enemy compromises and replicates a node and is in agreement with the witness nodes of that particular node, it can easily secure any number of the clone nodes. In this condition, the detection protocol is deficient. Therefore an optimum procedure should be non-deterministic and full distributed (NDFD), so as to detect the clone node in the mobile WSN reliable. The classification of the procedures is presented in table (1) according to these criterions.

2) Requirements of clone node detection procedures

Considering the studies conducted in different papers [7-20], and the inherent characteristics of the WSNs and the capabilities of the attacker, the analysis and classification of different procedures have been carried out according to the below criteria:

1. The procedure to be NDFD
2. The resistance capability against the smart attacker: in the smart attack, the enemy recognizes and inactivates the critical witness nodes (e.g. jamming). Thus for stopping the enemy from training the critical witness nodes, a security requirement should be designed, which by the detection protocol is fulfilled. The requirement: ***in each round for a node, all the nodes must have the same probability in order to be a witness node***. Besides, if the enemy is able to delete some of the nodes, it cannot obtain anything about the nodes that have high probability of being as witness nodes of a certain node.
3. Independent from the location information: Because the awareness of each node of its own location is a strict condition, to be independent from awareness location condition is important criteria of rationality of the detection procedure.
4. Communication and memory overhead: Regarding the extreme limitation of energy and hardware sources in WSNs, these criteria are also considered as an effective factor for rationality of the detection procedure.

Table1. Classification of node clone detection procedures

Procedure	NDFD	Resistance against smart attacker	Independent of location	Communication Cost	Memory Cost
XED[12]	Yes	No	Yes		
SDD[16]	Yes	No	Yes		
CDD[16]	Yes	No	Yes		
EDD[17]	Yes	No	Yes		
SEDD[17]	Yes	No	Yes		
ULTSE[14]	No	No	No		
MTLSD[14]	No	No	No		
SPRT[9]	No	No	No		
SHD[11]	Yes	Yes	Yes		
key Pre-Distribution[13]	No	No	Yes		
Patrol[18]	Yes	Yes	No		
Mobile-adversary[10]	Yes	No	Yes		

In table (1), it is observed that the optimum procedure that could fulfill all the security requirements for MWSNs is the SHD procedure. Because SHD is independent from the location information and in comparison with other procedure for network with big dimensions has lower communication and memory overhead. But generally, communication and memory overhead are medium and in order to $O(\sqrt{n})$. Therefore we can conclude that coming up with a full optimum procedure is one of the open discussions in this area; Besides, the need for presenting theoretical analyses and modeling in this area is extremely felt.

V. Conclusion

In this paper all procedures presented for the detection of replica node attacks in sensor networks with mobile nodes is reviewed and analysis. Also, by using mobility criteria, a new classification for node replica detection procedures and attacker model are proposed. To compare and evaluate different procedures, different metrics are introduced and used for theoretical analysis and classification procedures. Moreover, results of theoretical analysis and metrics are used for assessment procedures. Finally, the theoretical analyses of different approaches are discussed. Analysis results demonstrate that the procedures, based on location information (UTLSE, MTLSD, and SPRT) have a higher detection rate and low false alarm rate. But, here are two important notices; first, generally, due to the constraints of WSNs, access location information for all nodes is a strict assumption. Moreover, it can be seen that the energy overhead in this approach is too high. Therefore, regarding the theoretical analysis it can be seen that the SHD largely meets the criteria for a suitable solution and also shows good performance. However SHD energy consumption in large-scale WSNs still is high. Therefore, regarding limitations WSN, to achieve an optimal solution for node replica detection, there is an open area for researchers.

REFERENCES

[1] Chen et al, “Sensor Network Security: A Survey”, IEEE Communications Survey & Tutorials. Vol 11, No2, Second Quarter2009
[2] W.T. Zhu et al,” Detecting node replication attacks in wireless sensor networks: A survey”, Journal of Network and Computer Applications 35 (2012) 1022–1034
[3] Michael Riecker et al,” A Survey on Intrusion Detection in Wireless Sensor Networks”, Technical Report, SEEMOO-TR-2011
[4] V.Manjula et al,” Replication attack mitigations for static and mobileWSN” International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011
[5] S.K.Das et al, “A synopsis on node compromise detection in wireless sensor networks using sequential analysis”, Computer Communications 34 (2011) 2003–2012
[6] Roberto Di Pietro et al,” Securing Mobile Unattended WSNs against a Mobile Adversary”, IEEE 2010
[7] Bryan Parno et al,” Distributed Detection of Node Replication Attacks in Sensor Networks”, IEEE 2005
[8] Ming Zhang et al,” Memory Efficient Protocols for Detecting Node Replication Attacks in Wireless Sensor Networks” IEEE 2009
[9] Ho et al,” Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks Using Sequential Hypothesis Testing” IEEE Transactions on Mobile Computing, Vol. 10, No. 6, June 2011
[10]J.-W. Ho et al,” Distributed detection of mobile malicious node attacks in wireless sensor networks”, Ad Hoc Networks 10 (2012) 512–523
[11]YanYxainaxniga and et al,” Single Hop Detection of Node Clone Attacks in Mobile Wireless Sensor Networks”, 2012 International Workshop on Information and Electronics Engineering (IWIEE)
[12] Chia-Mu Yu et al,” Mobile Sensor Network Resilient against Node Replication Attacks” 2008 IEEE
[13] Deng XM, Xiong Y.” A new protocol for the detection of node replication attacks in mobile wireless sensor networks”, Journal of Computer Science and Technology 26(4): 732-743 July 2011. DOI 10.1007/s11390-011-1172-1
[14] Xiaoming Deng et al,” Mobility-assisted Detection of the Replication Attacks in Mobile Wireless Sensor Networks”2010 IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communication
[15] Mauro Conti et al,” Mobility and Cooperation to Thwart Node Capture Attacks in MANETs” EURASIP Journal on Wireless Communications and Networking Volume 2009, Article ID 945943, 13 pages
[16] Mauro Conti et al,” Emergent Properties: Detection of the Node-capture Attack in Mobile Wireless Sensor Networks” WiSec’08, March 31–April 2, 2008, Alexandria, Virginia, USA.
[17] Chia-Mu Yu et al,” Efficient and Distributed Detection of Node Replication Attacks in Mobile Sensor Networks” 2009 IEEE
[18] Liang-Min Wang et al,” Patrol Detection for Replica Attacks on Wireless Sensor Networks” Sensors 2011, 11, 2496-2504; doi:10.3390/s110302496
[19] Emil Selvan et al.,” Detection of Compromised Nodes in Mobile Ad-Hoc Networks”, Journal of Computational Information Systems 7:6 (2011) 1823-1829
[20] J.-W. Ho et al.,” Distributed detection of replica node attacks with group deployment knowledge in wireless sensor networks” Ad Hoc Networks 7 (2009) 1476–1488
[21] Mauro Conti,” Distributed Detection of Clone Attacks in Wireless Sensor Networks”, IEEE Transactions on Dependable and Secure Computing, VOL. 8, NO. 5, September/October 2011
[22]XiaoAmutihnogr et al,” A Replication Detection scheme for Sensor Networks”,rPinrogc 0e0d i(a2 E01n1g)i n0e0e0r–in0g0 02 9 (2012) 21 – 26
[23] Wen Tao Zhu,” Node Replication Attacks in Wireless Sensor Networks: Bypassing the Neighbor-Based Detection Scheme” 2011 International Conference on Network Computing and Information Security
[24]ChunmingRong,” An Efficient Intrusion Detection Scheme for Wireless Sensor Networks”, STA 2011 Workshops, CCIS 187, pp. 116–129, 2011
[25]Wang Liu, Kejie Lu et al,” Performance Analysis of Wireless Sensor Networks with Mobile Sinks” IEEE Transactions on Vehichular Technology, Vol. XX, No. YY, Month 2011
[26] Tamara Bonaci et al,” Distributed Clone Detection in Wireless Sensor Networks: An Optimization Approach” 2011 IEEE
[27] Abu Saleh Md. Tayeen et al,” Mobility Assisted Solutions for Well-known Attacks in Mobile Wireless Sensor Network”, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 9, No. 5, May 2011
[28] Thanh Dai Tran et al,” Early and Lightweight Distributed Detection of Node Replication Attack in Sensor Networks”, IEEE Communications Society subject matter experts for publication in the WCNC 2010 proceedings
[29] Tamara Bonaci et al,” Node Capture Attacks in Wireless Sensor Networks: A System Theoretic Approach”, IEEE2010
[30] Bin Tong ET AL,” A three-tier framework for intruder information sharing in sensor networks” Ad Hoc Networks 8 (2010) 345–360
[31] ShigenShen,” A game-theoretic approach for optimizing intrusion detection strategy in WSNs” 2011 IEEE
[32] AbderrezakRachedi,” muDog: Smart Monitoring Mechanism for Wireless Sensor Networks based on IEEE 802.15.4 MAC”, IEEE International Conference on Communications ICC2011 (IEEE ICC'11), Kyoto: Japan (2011)
[33] Noman Mohammed et al,” Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET” IEEE Transactions on Dependable and Secure Computing 2012
[34] Bo Zhu et al,” Localized Multicast: Efficient
And Distributed Replica Detection in Large-Scale Sensor Networks” IEEE Transactions on Mobile Computing, Vol. 9, No. 7, July 2010
[35] Muhammad Imran et al,” A Survey of Simulators, Emulators and Testbeds for Wireless Sensor Networks”, IEEE2010
[36] AnsgarKellner et al,” Simulation Environments for Wireless Sensor Networks” Technical Reports of the Institute of Computer Science at the Georg-August-University at Gottingen, June 2010
[37] C. Mallanda et al,” Simulating Wireless Sensor Networks with OMNeT++”, LSU Simulator, Version 1, 2005
[38] Xuedong Xian et al,” Comparison of OMNET++ and Other Simulator for WSN Simulation”IEEE2008
[39] Klaus Wehrle et al,” Modeling and Tools for Network Simulation”, Springer-Verlag Berlin Heidelberg 2010
[40] Roberto Di Pietro et al,” Intrusion-Resilience in Mobile Unattended WSNs” IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings
[41] Sooyeon Shin,” An Experimental Study of Hierarchical Intrusion Detection for Wireless Industrial Sensor Networks”, IEEE Transactions on Industrial Informatics, VOL. 6, NO. 4, NOVEMBER 2010
[42] P. Samundiswary et al,” Detection of Sinkhole Attacks for Mobile Nodes in Heterogeneous Sensor Networks with Mobile Sinks” International Journal of Computer and Electrical Engineering, Vol. 2, No. 1, February, 2010 1793-8163
[43] Mauro Conti,” The Quest for Mobility Models to Analyses Security in Mobile Ad Hoc Networks” WWIC 2009, LNCS 5546, pp. 85–96, 2009.
[44] MarjanKuchaki Rafsanjani et al,” Identifying Monitoring Nodes with Selection of Authorized Nodes in Mobile Ad Hoc Networks”, World Applied Sciences Journal 4 (3): 444-449, 2008
[45] Patrick Tague et al,” Modeling Node Capture Attacks in Wireless Sensor Networks”, IEEE 2008
[46] T. Bonaci et al.,” A convex optimization approach for clone detection in wireless sensor networks”, Pervasive and Mobile Computing (2012)
[47] N. Komninos et al. “Detecting unauthorized and compromised nodes in mobile ad hoc networks” Ad Hoc Networks 5 (2007) 289–298
[48] T. C. Lam et al,” A Mobile Agent Clone Detection System with Itinerary Privacy” Proceedings of the Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE’02)
[49] YingpeiZeng et al,” Random-Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks”, IEEE Journal on Selected Areas in Communications, Vol. 28, No. 5, June 2010
[50] Chia-Mu Yu et al, “CSI: Compressed Sensing-Based Clone Identification in Sensor Networks”, 8th IEEE International Workshop on Sensor Networks and Systems for Pervasive Computing 2012, Lugarno (19 March 2012)
[51] The IEEE 802.15.4 standard (ver. 2006) http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf
[52] A. Liu and P. Ning, “TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks,” in Proc. IPSN, Apr. 2008,pp. 245–256.
[53] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, “Energy analysis of public-key cryptography for wireless sensor networks,” in Proc. IEEE Int. Conf. Pervasive Comput. Commun., Mar. 2005, pp.324–328.

[54] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller,and M. Sichitiu, "Analyzing and modeling encryption overhead for sensor network nodes," in Proc. 2nd ACM Int. Conf. Wirel. SensorNetw.Applicat., 2003, pp. 151–159.

AUTHORS

First Author – Mohammad Hassan Ansari,MSc student, Iran University of Science and technology (IUST), mh_ansari@elec.iust.ac.ir

Second Author – Prof. VahidTabataVakily, Professor, Iran University of Science and technology (IUST), vakily@iust.ac.ir

Correspondence Author – Mohammad Hassan Ansari,MSc student, Iran University of Science and technology (IUST), mh_ansari@elec.iust.ac.ir,+982183857000