IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 2, November 2023

Recent Investigations in Wireless Sensor Networks on Distributed Defense Mechanism for Clone Attacks

Hemant Shakywar[1], Ashish Gupta[2], Anuradha Pathak[3]

Research Scholar, Department of Electronics & Communication [1]
Assistant Professor, Department of Computer Science and Engineering[2]
Assistant Professor, Department of Electronics & Communication[3]
Nagaji Institute of Technology & Management, Gwalior, India

Abstract: *Regarding accelerating development of mobile sensor nodes technology, increasing the utilization of them, and also facing with security challenges in these networks; specially clone nodes attack, this paper focuses on exploiting optimum criteria of node clone intrusion detection procedures in mobile wireless sensor networks by using experimental analysis of procedures. Since many of recommended protocols in this area have not been experimentalised, also no comprehensive study has been performed on the possibility and capability of these procedures; in this paper types of sensor network architecture, with the presence of mobile sensor node, are analyzed. Then according to the type of architecture, the procedures of clone node intrusion detection is classified and meticulously scrutinized. Besides, due to measuring the efficiency, exploiting the optimum parameters and also appraising the expenses of procedures, Finally, the conclusion based on theoretical analysis and simulation is presented.*

Keywords: wireless sensor network (WSN), clone attack, mobility.

I. INTRODUCTION

In recent years, the drastic advanced development in sensor node design reduces cost along with minimized hardware complexity. Sensor node is effective for deploying the field of WSN in distributed network with abundant nodes in self organized way. By considering several factors, deployment of sensor nodes is carried out with the factors like building structural integrity, pollution level in environment, surrounding brightness level, moisture in surrounding environment, building control factors etc. Other than development, sensor nodes are subjected to various security issues when deployed in Wireless Sensor Network (WSN) environment, since there are two existing kinds of threats like application dependent and application independent. Application independent attacks track objects in the field of battle, when WSN performs processes like synchronization, aggregation, localization, routing etc. Similarly, if WSN is deployed in the difficult environment like high heat, and humidity variation, then sensor nodes can easily capture and compromise those nodes and they can be used by hackers to interrupt operations.

Through compromised nodes, hacker can insert counterfeit data in the wireless network environment by means of the snoop. Also, by means of compromised nodes, hackers may perform clone attack in the network in the region of the key generation process of the wireless system. In clone type of attack, hacker generates replica nodes for the compromised nodes in the network through which the distribution system also shares key with the duplicated node and by means, the hacker may detect secret key of the system. By providing huge quality of replication nodes, WSN will be able to generate wider distribution system. This type of clone attack is also known as replication attack of the system which comes under the category of independent attack. Replication attacks are divided into two scenarios broadly which all state as replicated nodes are assumed that they are fully faithful to its corresponding nearby nodes. These nodes are not aware of replicated nodes, due to lack of counter measures factors and when the huge amount of compromise nodes are available, there is no need for examining a large number of nodes in the network. For detecting compromising node, single node is enough for examining cost and attack in the persistent environment and also clone generation is very cheap for network environment.

DOI: 10.48175/IJARSCT-13881

Furthermore, many conventional techniques have been proposed to recognize the duplicated nodes that are present in the literature review section. But they don't meet the necessities in identifying the attack. To address this issue, conventional technique named Intensified Randomized Efficient Distributed (IRED) has been proposed. The proposed research is carried out in two folds. To begin with, specialists have broken down the properties of the mechanism for detecting cloned nodes. Secondly, the survey results have suggested IRED protocol. The proposed protocol is the development of RED protocol. Here, we focused on preventing the clone attack to infest. In spite of the fact that the convention keeps the assault, few attacks penetrate into the system. In that situation, the duplicated nodes are detected by IRED. The empirical results show that the proposed protocol IRED has higher resistance against the assault and furthermore, performs better in view of amputation, memory and communication.

II. RELATED WORK

Anthoniraj et al. (2014) have enhanced remote sensor systems which are conveyed in threatening environment and defenseless against different sorts of assaults. In this work, they have sketched out the distinctive sorts of assaults on WSN and for the most part about clone assault where different ways are dealt to discover the cloned hub. In static unified conventions, CSI convention has the most minimal correspondence overhead than SET, real time and new conventions. In static disseminated conventions, it is found that SDC convention has lower correspondence than different conventions for littler size system and RED convention has the least correspondence overhead for bigger system. The SDC convention has lower memory overhead than the other conveyed conventions. The RED and BC-MEM conventions have preferred discovery likelihood over different onventions.

Ansari et al. (2018) have reviewed and analysed all the procedures presented for the detection of replica node attacks in Wireless Sensor Networks with mobile nodes. Also, by utilizing mobility criteria, a new classification for node replica detection procedures, an attacker model, is proposed. To compare and estimate different procedures, metrics are introduced and used for theoretical analysis and classification procedures. Moreover, results of theoretical analysis and metrics are used for the assessment procedures. Then, for a realistic assessment, different network layer protocols and constraints in WSN are considered. Finally, the theoretical analysis and simulation results of the performance of various schemes are discussed. Measurement results demonstrate that the procedures based on location information have a higher detection rate and low false alarm rate. But here, there are two important notices: first, generally, due to the constraints of WSNs, access location information of all nodes is a strict assumption. Moreover, it can be shown that the energy overhead in this scheme is too high. Hence, the simulation and theoretical analysis can be shown that SHD largely meets the criteria for a suitable solution and also shows better performance. However SHD energy consumption is still high in large-scale WSNs.

Chan et al. (2003) have that proposed the efficient bootstrapping of secure key is critical significance for secure sensor network applications. Local processing of sensor data needs secure node to node communication. In this work, three efficient random key pre-distribution methods are proposed for solving the security bootstrapping issue in resource-constrained sensor networks. Each of these three approaches represents various tradeoff in the model space of random key protocols. The choice of which approach is thebest for a given application will depend on which trade-off is the most appealing. The q-composite scheme obtains significantly enhanced security under small scale attack at the cost of greater vulnerability to large scale attacks. It increases attacker's cost of mounting an attack because the option of harvesting a number of keys in order to extract a random sample of the readings in the entire network is no longer appealing. So, it forces the attacker to act as a large scale node capture attack. The multipath reinforcement approach increases security at the cost of network communication. Since the expected number of common neighbors is proportional to n0 (where n0 is the expected number of neighboring nodes), this approach performs best, when the deployment density is distributed related to the communication radius of the nodes. It also presents the best characteristics, when the variation in deployment density is low. The random pairwise method has the best security properties of three schemes. It shows perfect resilience against node capture attacks and it also supports node based revocation and resistance to node replication. The characteristics come with the trade-off that the maximum supported network size is not as large as the other schemes.

Jagtap et al. (2019) have analyzed newly designed protocol for the detection of node replication attack which creates far difference such as energy utilization, memory overhead, detection probability, witness distribution, authentic and secure

DOI: 10.48175/IJARSCT-13881

detection compared to RED protocol. The proposed scheme has been extended to RED and it is more efficient, effective and accurate in detecting cloned node in WSN. This method improves the security of Wireless Sensor Networks mainly in unattended environment and improves the real time data acquisition systems.

Conti et al. (2006) presented a few common requirements for an ideal protocol for distributed detection of node replicas. In particular, in this work, they have introduced the preliminary notion of ID-obliviousness andarea-obliviousness that convey a measure of the quality of the node identity replicas detection algorithm; that is, it is resilience to an active attacker. Moreover, it is indicated that the overhead of such a protocol should be not only small, but also distributed among nodes. Otherwise, the protocol itself could sensibly impact. On the network life, the energy needed for the number of messages is exchanged and the computations are performed. On the effectiveness of the protocol, the memory has to exceed the storage available to the sensor. Finally, the proposed method has analyzed the state of the art solution for node identity replicas detection and also shown that the proposed solution does not completely fulfill the issues above described.

Koshy et al. (2013) have employed a Wireless Sensor Network (WSN) in an emerging area which has wide applications. Therefore, the security in WSN is great concern where node replication attack is an important attack against a WSN in which an adversary compromises a sensor node, produces copies of that node and are deployed it in strategic areas. Different methods have been developed to detect the node replication attacks. Zone based node replica detection using trust is an improved method which increases the packet delivery ratio and reduces the end to end delay.

III. METHODOLOGY

There are several benefits in the proposed system and it can be categorized for RM as well as for LSM. The primary notion of ID obliviousness and area obliviousness, which convey a measure of the quality of node replicas detection protocol, has been introduced that is, its resilience has smart adversary. Moreover, it has been indicated that the overhead of such a protocol should not be only small, but also evenly distributed among the nodes, both in computation and memory.

Consider a Wireless Sensor Network (WSN) consisting of set of nodes. These nodes may or may not be static. These nodes interconnect with all by sending claim message. Adversary captures the credential of compromised node and injects cloned hub into system. This clone hub can partake in communicating with other nodes as this node is going to be considered as unique hub and the clone hub is holding required credential. At least one clone node in network can fulfill adversary intention.

Wireless Sensor Network(WSN) comprises static and movable nodes which are used to communicate with each other or with base station for playing out certain operation. Base station or access point is considered to be utilized for putting away dispersed hub data table and used for broadcasting random value to other node. This distributed nodes data table holds the node data information of paired key value. Key is the ID of the node and the value is location of the node. Enemy assaults this system and catches qualifications and details of compromised node resulting cloned node. When any new or cloned node goes into system, emphasis of algorithm runs and checks the newly entered node’s ID against node data table. If the ID is present into table with incoherent location then revocation procedure is gets summoned for that node ID else calculation redesigns node information table with newly entered node.

Assured quantity of nodes is deployed in the network and they transmit their information to the sink node that gathers and then forwards it to the entrance point. These entrance focuses are responsible to have further communication with the base station and the destination hub, correspondingly. A simple yet powerful adversary threat model has been proposed. The characterized aggressors are conceivable to trade off a specific altered amount of nodes and replicate one alternately for various clones into the system. To handle with the threat, it would be probable to assume that nodes are tamper-proof. It has also been assumed here that the nodes are stationary and the adversary would be in and around the network environment such that they can pick up the entrance of access point closer to BS and launch clone attack. Then, the adversary can compromise single or couple of nodes through the cryptographic information of the compromised node and by which it produces the clone and embed into the system. The bargained as well as cloned nodes are fully organized by the opponent and can connect with each other at any time. By this way, the attacker changes the data that are required and send it to the entrance point. In this way, the focuses are made more intelligent to maintain a key separation from the invasion of an adversary. In the event that if the enemies are more powerful than the

DOI: 10.48175/IJARSCT-13881

forestalling strategy, the IRED drops its energy, from where the detecting component begins. The location system has the supposition that the goal of the enemy is to debilitate the discovery convention which is disseminated by compromising minimal subset X of the nodes. The adversary has collaborated 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 Pw (z) returns the probability that 2E INVY is a witness for the next run of the protocol. The following are the major requirements that ought to be met out by the conveyed discovery system,

- Overhead
- Witness distribution

3.1 Storage Overhead

It is often very hard to design protocol for the detection of such attack, because of the resource constraints of the sensor network. So, it is required to produce little overhead on the network. In addition to the above obligation, it also required to allocate the overhead to the entire network. Through the execution, it may be possible for a subset of entire node to experience much higher overhead. If such circumstance emerges, then the nodes present in the subset exhaust their energy quickly much higher overhead and it is more appropriate, when the memory is measured. When the memory overhead is higher for a subset of nodes in the system, then it might be feasible for these nodes to overflow. Amid overflow, it is unrealistic for the hub to execute the protocol. These requirements implicitly express that the overhead formed by the sensing protocol should be small and distribute evenly among the nodes.

3.2 Witness Distribution

Choosing witnesses for identifying the clone assault is the major issue in WSN. If an attacker is able to detect the future observers before the identification convention 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.

3.3 Location-based prediction

The probability of a witness node does not rely on the land area of the relating node.

3.4 ID-based prediction

The protocol does not provide any information about the ID of a node in the network and it may be the witness for the protocol for the next run.

IV. IRED PROTOCOL BEFORE INFUSING (PREVENTION)

The attackers can be blocked, if the access-point is more astute and that is capable of delaying the correspondence or accepting the data from original and cloned nodes. The suppositions made on access-point get or accept the data packets from the original and malicious nodes at different time and the access-point gets or acknowledges the information packages from unique and malicious nodes at various time of interim. The points of interest of those information packets are recorded in the data base. The variation in the recorded points of interest makes perplexity to users. Then, access-point is able to block the communication nodes with same ID. Then, it can expel struggle ID and information from the node and also, announces all the nodes about the occurrence of replication. So as to get access to the point, an attacker usually tries to insert the cloned node through the middle of the road nodes of the system by a multi-bounce communication. In such a scenario, if there is no proper redesigns for the hubs in the system. They are most certainly not ready to have clear thought of the new nodes passage. In this situation, the WED protocol of prevention strategy is distributed among the nodes that approve and keep the new section of nodes in light of few obliges. Along these lines, the cloned nodes are removed at the access-point itself without influencing the correspondence among unique, honest and goodness of nodes.

V. AFTER PENETRATION (DETECTION)

In case, if the opponents are more intense than staying away from the technique, IRED drops its energy from where the recognizing system starts. Two steps are solved in recognition of clone assault. At the initial step, among the nodes of

DOI: 10.48175/IJARSCT-13881

the network, a random value is shared. This value is then shown with a brought together instrument. Once the random value is shared successfully among the nodes, then the second step on location of the clone hub is resolved. In the second step each node signs digitally and broadcasts the geographic location and the case ID. On getting the telecast message, they guarantee a subset of network locations that are selected pseudo randomly. If a claim is sent to a node's ID and that is no longer alive in the network, then such claims are lost. First deployed nodes are alone considered for witness. WED can easily adapt to work, when a particular node is used as the message destination. For the detection purpose, it has been 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 comes up short and sending message is not influenced by wormhole attack or by dropping. Moreover, adversaries are capable to control the witness set. In any case, it expands more time to compromise those nodes because reaching them the recognizable proof tradition is successfully kept away from it.

The major issue that gains more attention from the identification system is the capacity. The location protocol requires certain amount of memory of all the nodes with a specific end goal to execute in the relating system. It is more important that the detection protocol should utilize less memory to get performed in the nodes, since the sensor nodes are normally resource constraints. Figure 3.1 explains the capacity overhead brought out by IRED and RED location convention. It stands evident for IRED that it needs very less memory also, causes low overhead on the sensor nodes. Subsequently, IRED outperforms RED in terms of storage requirements.

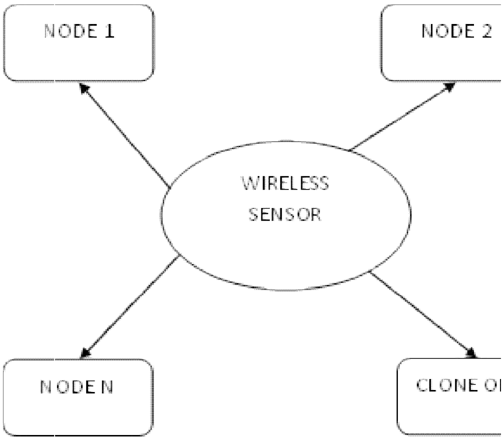

Figure 1 Sensor network design for level 0

VI. PACKET DELIVERY RATIO (PDR)

Packet Delivery Ratio (PDR) is another important factor which portrays the parcel convey and proportion of the hubs in the system while executing the detection algorithm. Similarly, it shows that the quantity of parcels conveyed to the sink nodes is higher for IRED protocol even when traffic rises, while comparing with RED protocol. It clearly denotes that IRED convention has less calculation overhead than the RED protocol. Consequently, it can be executed effectively in the sensor networks.

6.1 Detection Efficiency

Efficiency of a convention in identifying the clone assault relies on upon the thickness of the movement and number of nodes in the sensor network.

DOI: 10.48175/IJARSCT-13881

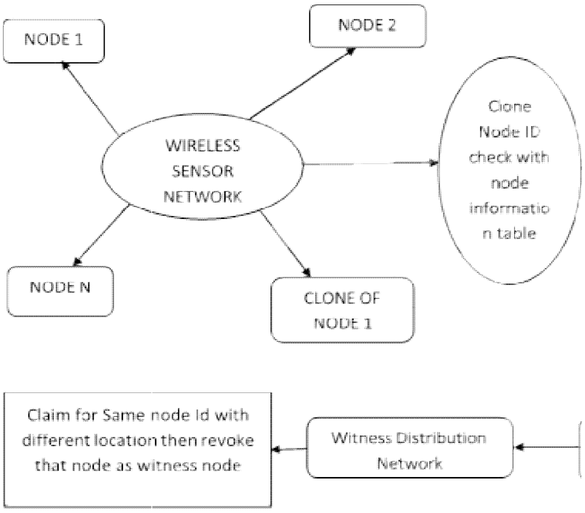
NODE 1
NODE 2
WIRELESS SENSOR NETWORK
Clone Node ID check with node information table
NODE N
CLONE OF NODE 1
Claim for Same node Id with different location then revoke that node as witness node
Witness Distribution Network

Figure 2 Sensor network design for level 1

Figure 2 shows the efficiency of the proposed algorithm in deciding the clone assault at different activity thickness. It additionally communicates that the location effectiveness of IRED convention is higher than RED convention, at first, while the traffic is lesser. If there is an occurrence of IRED, the recognition adequacy is unfaltering up to 40% and begins diminishing only after the traffic density increases >40%.Detection productivity is additionally, influenced by the quantity of nodes in the network and it represents the detection capacity of the conventions of various number of nodes in the system. It is evident that RED protocol performs better only at the point when there is extensive numbers of nodes, though the recognition effectiveness is ordinary, when the quantity of nodes lesser. In IRED protocol, as the number of nodes increases, the identification of effectiveness also increases.

6.2 True positive

It is necessary to find the attack correctly, and the typical operations should not be distinguished as the clone attack. It represents that IRED identifies the clone assaults more accurately than RED protocol.

VII. RESULT AND DISCUSSION

For this simulation, 800 nodes in WSN and communication radius as 0.2 are considered. The nodes are uniformly distributed in the network at unsystematic manner. The performance of IRED is computed for the storage, detection accuracy, Packet Delivery Ratio and true positive.

7.1 Storage Overhead

The major problem that gains more attention from the detection approach is storage. The detection protocol needs certain amount of memory of all the nodes in order to execute in the corresponding networks. It is more important that the detection protocol should utilize less memory to get executed in the nodes, since wireless sensor nodes are normally resource constraints. Figure 3 and Table1 explain the storage overhead caused by the RED protocol and IRED detection protocol. It is the fact that IRED requires very less memory and causes much low overhead on the sensor nodes. Hence, IRED outperforms RED in terms of storage requirements.

Table 1 Storage overhead

Simulation time (msec)	RED(mb)	I-RED(mb)
0	90.5	95.7
10	91.5	96.5
20	92.5	97.4
30	92	98.5
40	94	99

DOI: 10.48175/IJARSCT-13881

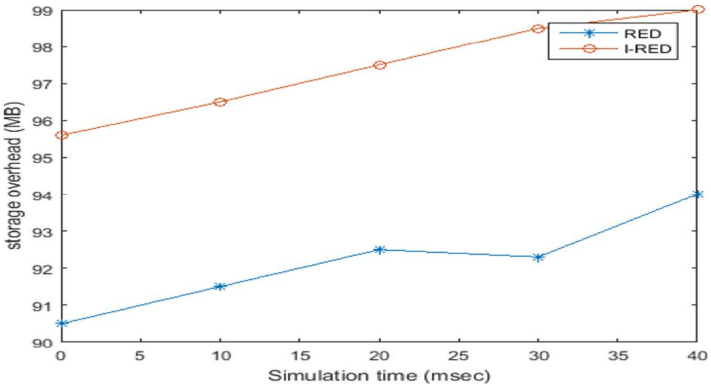

Figure 3 Storage overhead

7.2 Detection Efficiency

Efficiency of a protocol in detecting the clone attack depends on the traffic density and number of nodes in the sensor network.

Table 2 Traffic density vs detection efficiency

Traffic density (%)	RED (%)	I-RED(%)
20	100	100
30	100	99.9
40	100	99.8
50	99.92	99.6
60	99.85	99.4

Table 3 Number of nodes vs detection efficiency

No. of nodes	RED (%)	I-RED(%)
0	97.52	99.6
10	97.55	99.6
20	97.55	99.61
30	98.1	99.7
40	98.1	99.8

Figure 4 expresses the efficiency of the proposed algorithm in estimating the clone attack at various traffic densities. It also expresses that the detection efficiency of IRED protocol is higher than RED protocol. Initially, when the traffic is lesser (i.e. <20%) the detection rates of both RED and IRED are the same. When the traffic increases (i.e. >20%), the performance of the RED protocol decreases gradually. In IRED, the detection efficiency is constant up to 40% and starts decreasing only after the traffic density increases >40%.

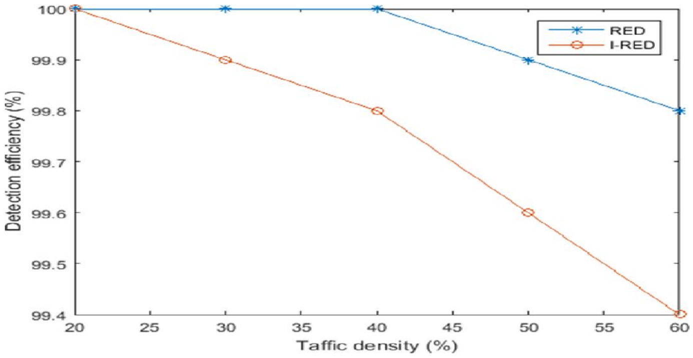

Figure 4 Traffic density vs detection efficiency

DOI: 10.48175/IJARSCT-13881

Detection efficiency is also, affected by the number of nodes in the network. Figure 5 represents the detection capacity of the protocols of different numbers of nodes in the sensor network. It is the fact that RED protocol performs better only when there is large number of nodes, where as the detection efficiency is normal when the number of nodes are lesser. For IRED protocol, the detection efficiency increases, when the number of node increases successively.

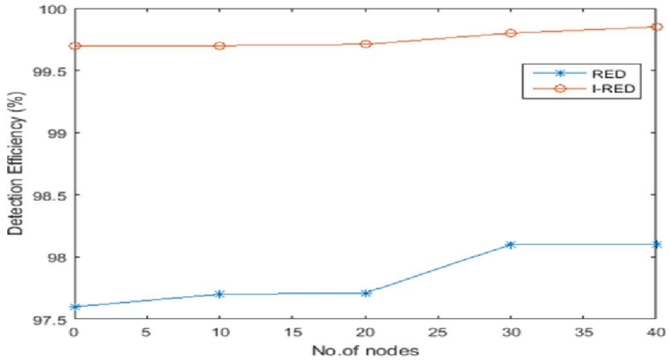

Figure 5 Number of nodes vs detection efficiency

7.3 Packet Delivery Ratio

Delivery ratio is more essential factor in WSN. As the sensor nodes are normally deployed with much less storage capacity, they may drop the packets, when they are overloaded. So, the design of the detection protocol should not overload the nodes. It is also shown that the number of packets delivered to the destination node is higher for IRED protocol even when the traffic increases compared to RED protocol. It explicitly indicates that the IRED protocol has less computation overhead than the RED protocol. Therefore, it can be implemented effectively in the sensor networks. Figure 6 and Table 4 show the packet delivery ratio versus traffic delivery ratio.

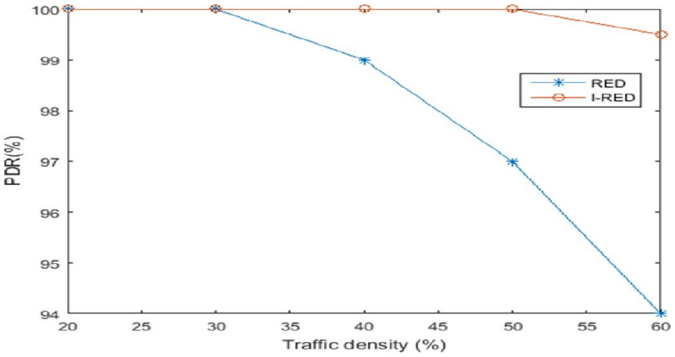

Figure 6 Packet delivery ratio Table 4.4 Packet delivery ratio

Table 4 Packet delivery ratio

Trafficdensity (%)	RED(%)	I-RED(%)
20	100	100
30	100	100
40	99	100
50	97	100
60	94	99.5

7.4 True Positive

It is essential to find the attack correctly where the normal procedures could not be detected as the clone attack. Figure 7 and Table 5 show the true positive comparison of RED and IRED where IRED detects the clone attacks much accurately than RED protocol.

DOI: 10.48175/IJARSCT-13881

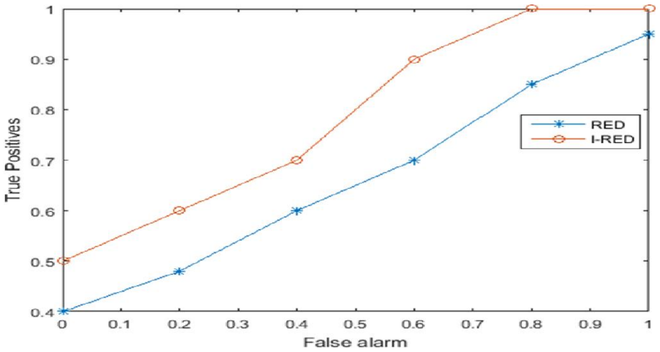

Figure 7 True positive

Table 5 True positive

Truepositive	RED	I-RED
0	0.5	0
0.2	0.6	0.4
0.4	0.7	0.58
0.6	0.9	0.7
0.8	1	0.87
1	1	0.93

VIII. CONCLUSION

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

This protocol initially prevents the attack which exists in the network. Prevention technique monitors the penetration of attack in the access-point of the network. Though the detection algorithm effectively blocks the attack earlier, some effective adversary may break the prevention technique and pervade into the network. Such pervade attacks are detected by using the detection technique. It determines the existence of the attack from the witness node. The efficiency of the Proposed IRED protocol is experimented in terms of storage overhead and detection capacity of the network.

REFERENCES

[1] Abbas, S, Merabti, M & Llewellyn-Jones, D 2009, 'Signal strength based sybil attack detection in wireless ad hoc networks', IEEE in Proceedings of the 2nd International Conference on Development in eSystems Engineering (DESE '09), Abu Dhabi, UAE, pp. 190-195.

[2] Akyildiz, IF &Kasimoglu IH 2014, 'Wireless sensor and actor networks: Research challenges', Journal of Ad Hoc Networks, vol. 2, no. 4, pp. 351-367.

[3] Akyildiz, IF, Su, W, Sankarasubramaniam, Y &Cayirci, E 2002, 'Wireless sensor networks: A survey', Int'l J. Computer and Telecomm. Networking, vol. 38, no. 4, pp. 393-422.

[4]Akyildiz, IF, Su, W, Sankarasubramaniam, Y &Cayirci, E 2018, 'Wireless sensor networks: A survey', Journal of Computer Networks, vol. 38, no. 4, pp. 393-422.

[5]Akyildiz, IF, Su, W, Sankarasubramanian, Y &Cayirci, E 2002, 'A survey on sensor networks', IEEE Communications Magazine, vol. 40, no. 8, pp. 102-114.

[6]Amuthavalli, R &Bhuvaneswaran, RS 2018, 'Detection and prevention of sybil attack in wireless sensor network employing random password comparison method', Journal of Theoretical and Applied Information Technology, vol. 67, no. 1, pp. 236-246.

DOI: 10.48175/IJARSCT-13881

ISSN 2581-9429 IJARSCT

[7]Anand, DG, Chandrakanth, HG &Giriprasad, MN 2012, 'Security threats & issues in wireless sensor networks', International Journal of Engineering Research and Application, vol. 2, no. 1, pp. 911-916.

[8]Anderson, R & Kuhn, MG 1996, 'Tamper resistance-A cautionary note', In Proceedings of the second Usenix workshop on electronic commerce, vol. 2, pp. 1-11.

[9]Ansari, MH &Vakili, VT 2018, 'Performance analysis and classification of clone attack detection procedures in mobile wireless sensor networks', International Journal of Computer Applications, vol. 71, no. 21, pp. 5-12.

[10]Anthoniraj, J & Abdul Razak, T 2015, 'NBCAD: neighbor based clone attack detection in cluster based static wireless sensor networks',. vol. 7, no. 3, pp. 912-921

[11]AymanTajeddine, AymanKayssi, Ali Chehab&ImadElhajj 2014, 'Authenticaton schemes for wireless sensor networks', 17th IEEE Mediterranean Electrotechnical Conference, Beirut, Lebanon, pp. 367- 372.

[12]BabuKarupppiah, A & Raja Pradash, A 2014, 'Sybilsecure: An energy efficient sybil attack detection technique in wireless sensor network', International Journal of Information Scinces and Techniques (IJIST), vol. 4, no. 3, pp. 107-113.

[13]Baig, ZA 2011, 'Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks', Computer Communications, vol. 34, no. 3, pp. 468-484.

[14]Balachandaran, N &Sanyal, S 2012, 'A review of techniques to mitigate sybil attacks', International Journal of Advanced Networking and Applications, vol. 4, pp. 1-6.

[15]Becher, Z, Benenson&Dornseif, M 2006, 'Tampering with motes: Real-world physical attacks on wireless sensor networks', Springer Berlin Heidelberg. Proc. International Conference on Security in Pervasive Computing (SPC '06), pp. 104-118.

[16]Bekara, C & Laurent-Maknavicius, M 2007, 'A new protocol for securing wireless sensor networks against nodes replication attacks', In Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMOB 2007), pp. 59- 59.

[17]Bettstetter, C & Hartmann, C 2015, 'Connectivity of wireless multihop networks in a shadow fading environment', Wireless Networks, vol. 11, no. 5, pp. 571-579.

[18]Blundo, C, De Santis, A, Herzberg, A, Kutten, S, Vaccaro, U & Yung, M 1992, 'Perfectly-secure key distribution for dynamic conferences', Springer Berlin Heidelberg in Annual International Cryptology Conference, pp. 471-486.

[19]Bonaci, T, Lee, P, Bushnell, L &Poovendran, R 2011, 'Distributed clone detection in wireless sensor networks: An optimization approach', IEEE In IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 1-6.

[20]Bonaci, T, Lee, P, Bushnell, L &Poovendran, R 2013, 'A convex optimization approach for clone detection in wireless sensor networks', Pervasive and Mobile Computing, vol. 9, no. 4, pp. 528-545.

[21]Brooks, R, Govindaraju, PY, Pirretti, M, Vijaykrishnan, N &Kandemir, MT 2007, 'On the detection of clones in sensor networks using random key predistribution', IEEE Transactions on Systems, Man and Cybernetics, Part C: Applications and Reviews, vol. 37, no. 6, pp..1246-1258

[22]Capkun, S &Hubaux, JP 2005, 'Secure positioning of wireless devices with application to sensor networks', IEEE In Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, pp. 1917-1928.

[23] Caruso, A, Chessa, S, De, S &Urpi, A 2005, 'GPS free coordinate assignment and routing in wireless sensor networks', IEEE In Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 1, pp. 150-160.

[24]Chan, H, Perrig, A & Song, D 2003, 'Random key predistribution schemes for sensor networks', IEEE Proceedings 2003 Symposium on Security and Privacy, pp. 197-213.

[25]Chen, G, Branch, JW & Szymanski, BK 2005, 'Local leader election, signal strength aware flooding, and routeless routing', IEEE in Proceeding of IEEE International Parallel and Distributed Processing Symp. (IPDPS '05), pp. 1-8.

[26]Choi, BG, Cho, EJ, Kim, JH, Hong, CS & Kim, JH 2009, 'A sinkhole attack detection mechanism for LQI based mesh routing in WSN, International Conference on Information Networking ICOIN, pp. 1-5.

DOI: 10.48175/IJARSCT-13881

[27]Choi, H, Zhu, S & La Porta, TF 2017, 'SET: Detecting node clones in sensor networks', IEEE In Secure Comm 2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops, pp. 341-350.

[28]Choi, H, Zhu, S & La Porta, TF 2007, 'SET: Detecting node clones in sensor networks', IEEE In Third International Conference on Security and Privacy in Communications Networks and the Workshops, September, pp. 341-350.

[29]Cocks, C 2001, 'An identity based encryption scheme based on quadratic residues', Springer Berlin Heidelberg In IMA International Conference on Cryptography and Coding , pp. 360-363.

[30] Conti, M, Di Pietro, R & Mancini, LV 2006, 'Secure cooperative channel establishment in wireless sensor networks', IEEE In Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'06), pp. 327-331.

[31]Conti, M, Di Pietro, R & Mancini, LV 2007, 'ECCE: Enhanced cooperative channel establishment for secure pair-wise communication in wireless sensor networks', Ad Hoc Networks, vol. 5, no. 1, pp. 49- 62.

[32]Conti, M, Di Pietro, R &Spognardi, A 2020, 'Clone wars: Distributed detection of clone attacks in mobile WSNs', Journal of Computer and System Sciences, vol. 80, no. 3, pp. 654-669.

[33]Conti, M, Di Pietro, R, Gabrielli, A, Mancini, LV & Mei, A 2019, 'The quest for mobility models to analyse security in mobile ad hoc

[34]Conti, M, Di Pietro, R, Mancini, L & Mei, A 2011, 'Distributed detection of clone attacks in wireless sensor networks', IEEE Transactions networks', Springer Berlin Heidelberg In International Conference on Wired/Wireless Internet Communications, May, pp. 85-96.on Dependable and Secure Computing, vol. 8, no. 5,pp. 685-698.

[35]Conti, M, Di Pietro, R, Mancini, LV & Mei, A 2006, 'Requirements and Open Issues in Distributed Detection of Node Identity Replicas in WSN', IEEE In 2006 IEEE International Conference on Systems, Man and Cybernetics, vol. 2, pp. 1468-1473.

[36]Conti, M, Di Pietro, R, Mancini, LV & Mei, A 2017, 'A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks', ACM In Proceedings of the 8th ACM International Symposium on Mobile ad hoc Networking and Computing, September, pp. 80-89.

DOI: 10.48175/IJARSCT-13881