International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. Journal Indexed in JIR, DIIF and SJIF.
Research Paper
Available online at: www.jrrset.com
UGC Approved Journal No: 45483
Received on: 05.12.2017 Published on: 29.12.2017 Pages : 28-34

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105
Volume 5, Issue 12
December 2017.
JIR IF : 2.54
DIIF IF : 1.46
SJIF IF : 1.329

ROUTING ATTACKS ON STATIC AND MOBILE WSN – A REVIEW

S.Saravanan, K.Richard
Department of Electronics and Communications Engineering
Dhanalakshmi Srinivasan Engineering College, Tamil Nadu, India

Abstract

Security is essential factor for quite a few sensor network applications. Wireless sensor Networks (WSN) when deployed in hostile environments as static or mobile, an antagonist will attempt to bodily seize some of the nodes, as soon as a node is captured, it collects all the credentials like keys and identity etc. the attacker will re-program it and repeat the node so as to structure replicas and pay attention the transmitted messages or regulate the functionality of the network. Identity criminal ends up in 2 sorts attack: clone and Sybil. In especially a catastrophic attack in opposition to sensor networks at any place one or more node(s) illegitimately claims an identification as replicas is recognized as the node replication attack. The replication assault is noticeably injurious to many essential functions of the sensor network like routing, useful resource allocation, misbehavior detection, etc. This paper look at the risk posed by way of the replication assault and a variety of other novel methods to discover and keep adjoining to the replication attack, and considers their effectiveness in each static and cellular WSN.

Keywords

Security, Clone, Sybil, node replication assault and static WSN.

1. INTRODUCTION

A Wireless sensor Network (WSN) can also be assortment of sensors with restrained resources that collaborate so as to gain a frequent goal. Sensor nodes operate in belligerent environments like hostilities fields and scrutiny zones. Due to their operative nature, WSNs are usually neglected, hence at chance of many varieties of novel attacks. The mission-critical nature of sensor community applications implies that any cooperation or defeat of sensory reserve due to a malicious assault launched by way of the adversary-class will cause considerable harm to the whole network. Sensor nodes multiplied in a battlefield ought to have wise adversary's operative in their surroundings, intending to subvert damage or hijack messages exchanged within the network. The agreement of a sensor node will end result in larger harm to the network. The wealth challenged nature of environments of operation of detector nodes in most cases differentiates them from distinct networks. All safety speedy restore proposed for sensor networks want to function with minimal energy usage, while securing the network. The basic safety necessities of WSN are ease of use, discretion, reliability and messages [16]. We classify detector community assaults into 3 essential classes [7] [8]: Identity Attacks, Routing Attacks &amp; Network Intrusion. Identity attacks intend to steal the integrity of legit node in operation inside the sensor network. The pinpoint attacks are Sybil assault and Clone (Replication) attack. In a Sybil attack, the WSN is superseding with the aid of a malicious node that forges an outsized range of faux identities so as to disrupt the network's protocols. A node replication assault is an attempt by using the adversary to add one or additional nodes to the community that use identical ID as every other node within the scenario.

Routing attack will location the rogue nodes on a routing path from a source to the base station should attempt to tamper with or discard professional data packets. A number of the routing assaults are sinkhole Attack, False routing data attack, Selective forwarding attack, and Wormholes. The antagonist creates an outsized sphere of influence, which can entice all visitors destined for the base station from nodes which may be many hops away from the compromised node that is regarded as sinkhole attack. False routing attack means interjecting false direction-finding arrange packets into the system. Concession node may also waste to forward or forward selective packets known as Selective forwarding attack. Within the wormhole attack, 2 or more malicious colluding nodes create greater stage virtual tunnel within the community that is employed to cross packets between the tunnels end points. Network intrusion is an unauthorized entrance to organism by each an exterior perpetrator, or by way of an insider with insignificant privileges. In this paper we are focuses on an individuality assault usual as replication assault wherever one or more nodes illegitimately hold an individuality of realistic node and replicated in entire WSN network as shown Figure 1. Reason for choosing this assault is that it will form the foundation of a range assaults such Sybil attack, routing assaults and link layer attacks, also recognised as denial of provider assaults that affects availability of network.

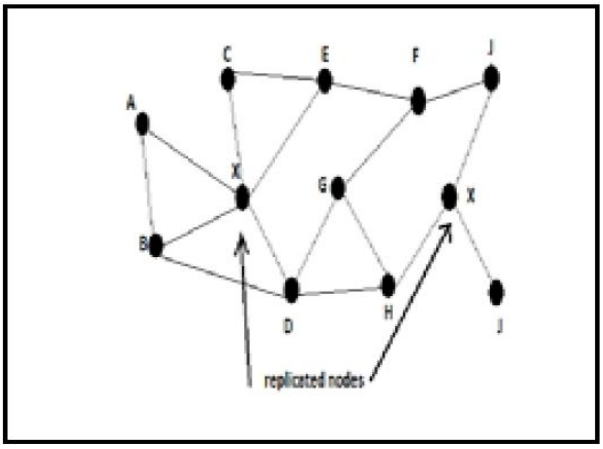

Fig.1 : Replication Attack

The attention of node replication attacks in a wi-fi antenna network is so a indispensable problem. Some centralized and circulated explanations have solely just been recommended.

Though, these options are now not gratifying. First, they are energy and reminiscence stringent: a considerable disadvantage for any protocol that is to be used in aid restricted environment like a sensor network. Further, they're inclined to precise adversary models brought in this paper.

Significance of Replication Attack and Background

Node Replication Attack: Wireless gadget network, companion character 1st bodily captures solely one or few of appropriate nodes, then clones or replicates them fabricating these replicas have the comparable persona (ID) with the imprison node, and ultimately expands a capricious quantity of clones all through the community reason of node replication attack are as follows:

It creates a giant injury to the community as a end result of the replicated node also has the equal identification because the professional member. It creates a range of attacks by way of extracting all the key credentials of the captured node. It debases the monitoring operations by way of injecting false data. It will reason jamming within the network, rattle the operations within the network and additionally initiates the Denial of Service (DoS) attacks too. It is hard to tell apart replicated node and consequently authentication is difficult. A WSN is both stationary or mobile. In static wireless sensor networks (SWSNs), the sensor nodes are stationary or static; that's, the system nodes are use at random, and as soon as deployment their positions do no longer diversity. On the similarly hand over, in transportable wireless sensor networks (MWSNs), the sensor nodes will bypass on their own, and once readying, displaying at absolutely different| areas at extraordinary times. The advantages encompass 1) localized detection; 2) effectiveness and efficiency; 3systemwide employer avoidance; and 4) network-wide revocation avoidance.

2. DETECTION METHODS

Supported on the detection methodologies, categorize the clone attack detection.

1. Detection Techniques for Stationary WSNs
2. Detection Techniques for Mobile WSNs

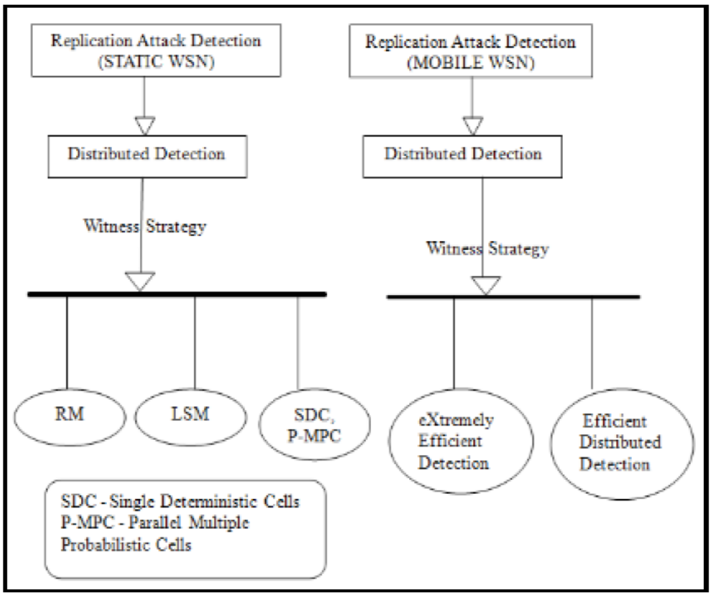
Replication Attack Detection (STATIC WSN)
Replication Attack Detection (MOBILE WSN)
Distributed Detection
Distributed Detection
Witness Strategy
Witness Strategy
RM
LSM
SDC, P-MPC
eXtremely Efficient Detection
Efficient Distributed Detection
SDC - Single Deterministic Cells
P-MPC - Parallel Multiple Probabilistic Cells

Fig. 2 : Steps of replication attack detection

Witness-decision line of attack- Node transmit its position maintain to its nationals, shares a nodes position maintains with a partial set of chosen witness nodes. Checking whether or not there are the similar ID's used at diverse position to sense the replicas. Static networks trust on the witness-finding technique that cannot be applied to mobile networks.

1 Detection Techniques For Stationary WNS's

The detection of node replication attack in static WSNs is categories in the main into 2 sorts as centralized and distributed methods.(A) Centralized methods: In integrated methods base position is consider to be a strong central that is responsible for info convergence and decision making. During the detection growth every node within the network sends its location allegation (ID, Location Info) to base station (sink node) through its neighboring nodes. Upon receiving the complete location allegation, the bottom station checks the node Ids on their location, and if it finds 2 locations with constant ID, it hikes a clone node.

(A.1)Random Key Pre-distribution:

the basic plan is that the keys used consistent with the random key pre distribution scheme should follow a certain pattern and those keys whose convention go above a threshold can be evaluator to be replica. Inside the protocol, numeration Blossom filters is used to collect key usage statistics. Every node makes a counting Blossom filter of the keys it uses to communicate with near nodes. It appends a random number (nonce) to the Blossom filter and encrypts the result using foundation position communal key; this encrypted data organization is forwarded to base station. Base station decrypts the Blossom filters it receives, discards duplicates, and polls the number of time every key used in the network. Keys used above a threshold expense are considered cloned. Base station makes a blossom filter from the cloned keys, encrypts the list using its furtive key and broadcasts this filter to the sensor network adopting a gossip protocol. Every node decrypts base stations blossom filter removes cloned keys from its keying, and terminates connections using cloned keys.

(A.2) SET:

The network is randomly divided into exclusive subgroup. Each of the subsets includes a subspace leader, and members are one hop removed from their subgroup leader. Multiple roots are randomly set to construct multiple sub trees, and each subgroup is a node of the subtree. Each subgroup leader collects member information and forwards it to the root of the subtree. The crossing operation is performed on each root of the subtree to detect replicated nodes. If the crossing of all subsets of a subtree is vacant, there aren't any clone nodes during this sub tree. In the end, every root ahead its information to the foundation station (BS).The base station detects the clone nodes by computing the crossing of any 2 received sub trees. SET identify clone nodes by causing node info to the bus from set leader to the root node of a randomly created sub tree and so to the BS.

(B) Distributed Techniques:

Distributed techniques consist no essential ability exists, and particular exposure method known as claimer-reporter-witness is provided within which the recognition is performed by nearby circulated node transfer the location claim to not the bottom station (sink) however to a randomly selected node known as witness node.

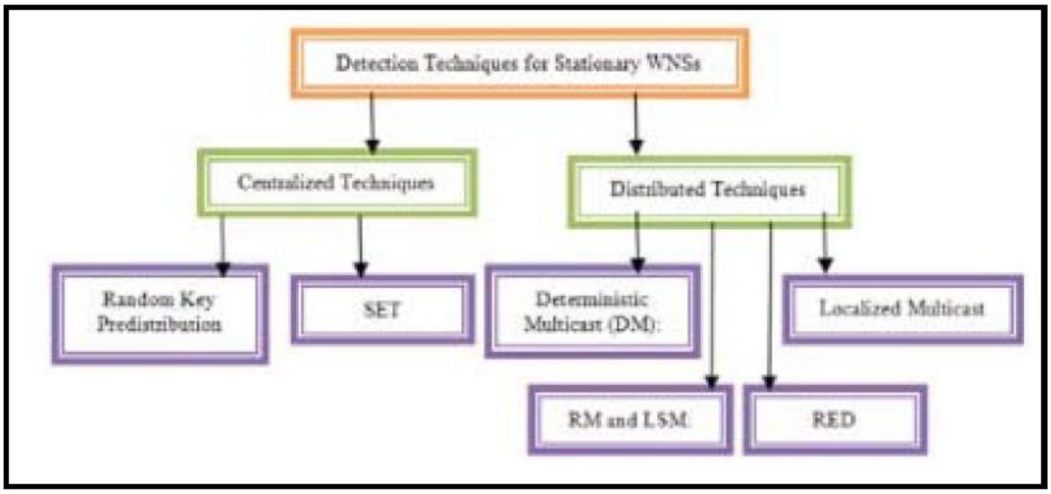
Detection Techniques for Stationary WNSs
Centralized Techniques
Distributed Techniques
Random Key Predistribution
SET
Deterministic Multicast (DM)
Localized Multicast
RM and LSM
RED

Fig.3 Detection techniques for stationary WSN

(B.1)Deterministic Multicast (DM): DM protocol could be a claimer-reporter-witness framework. The claimer could be a node that domestically broadcasts its location claim to its neighbors, every neighbor small indefinite amount as a communicator, and employ operate to map the claim ID to a witness. Then the neighbor forwards the claims to the witness, which is able to receive 2 completely different location claims for constant node ID if the antagonist has replicated a node. One drawback will occur that the antagonist may also use operate to understand concerning the witness for a given claim ID, and will find and compromise the witness node before the antagonist inserts the replicas into the WSN therefore on evade the detection.

(B.2) RED: Irregular, efficient, and distributed protocol known as RED, for the detection of node replication attack. It assassinates at fastened intervals of your time and consists in 2 steps. In beginning, a random worth, randomly, is shared between all the nodes through base station. Succeeding step is termed detection section. During this section, every node broadcasts its claim (ID and location) to its neighboring nodes. Every neighbor node that hears a claim sends (with likelihood p) this claim to a collection of pseudo every which way elite network locations. The pseudo random operate is taking as associate input ID, random range. Each node within the pathway (from claim node to the witness purpose) onwards the message to its neighbor nearest to the destination hence, the replicated nodes is going to be detected in every detection step. Once next time the RED executes the witness nodes are going to be take issue since the random worth that is broadcasted by the bachelor's degree is modified.

3. OBJECTIVE

An objective of this thesis work is as follow:

- ❖ The study target analysis of WSN Routing Protocol.
- ❖ Prepare the Wireless sensing element Network (WSN) state of affairs with simulation time of ten0sec with 10 nodes, fifteen nodes and twenty nodes.
- ❖ Analyzing the consequences of residual energy, throughput, normalized routing load and network lifespan in WSN state of affairs with completely different atmosphere.
- ❖ Analyzing the results of AODV, AMODV protocols to investigate that one style of protocol provides higher performance.

4. PROPOSED ALGORITHMIC PROGRAM

The planned algorithmic program is predicated on the trust values of individual nodes. All the nodes of wireless ad-hoc network have a particular trust worth. The algorithmic program encompasses the subsequent steps:

[A] Initialization:

1. Trust values of all the collaborating nodes square measure set to be initialized by specific previously assigned trust value.

2. Initialize the trust value of every node with 100.

3. Assumption: 1 trust value = 10 packets dropped.

[B] Updating of hope values:

1. If the packs are properly pass on from one node to another node:

(a) If the correctly transmitted no of packets is between 1 and 10, then trust values of the respective nodes will be incremented by one time. Updated trust value = old trust value + 1;

(b) If the correctly transmitted number of packets is greater than 10, then the updated trust value will be: Updated trust value = old trust value + (properly pass on packs / 10);

2. If the packets are dropped/delayed (a) The number of dropped or delayed packets is between 1 and 10and then trust value of that particular node is decremented by one. Renew trust value = old trust value – 1;

(b) The numeral of dropped or delayed packets are greater than 10, then hope value of that exacting node will be,

Renew trust value = old trust value – (Packet dropped or delayed / 10);

1. If the hope value of exacting node is depressing, next print “Invalid node”. [C] Isolating the Packet drop node as of the system

1. If (renew trust value < Threshold trust value) Then the particular node is treated as malicious node (Black hole node)

2. If (Updated trust value > Threshold trust value) Then the particular node is treated as legitimate node. Stop comparing the trust values of nodes with threshold.

5. CONCLUSION

In this paper we discussed classification of detection mechanisms for replication attack in static WSN. Distributed detection approach is additional advantages than centralized approaches since single point failure. In witness supported strategy of circulated come up to, uncertainty introduced in selecting witnesses at varied levels like whole network and restricted to geographical grids to avoid prediction of future witnesses. If chosen witness node itself cooperation node or replica node then recognition of replication attack is uncertain. There is also trade-off between communication charge visual projection and recognition time. All the approaches dealt with static WSN. With the deployment information (like order, neighbourhoods, and group members with locations) all the nodes within the network should recognize highest deployed generation that impractical and cannot move a part of alternative teams since neighbours or fingerprints vary. Some WSN application needs mobile nodes. The complete access become complex once considering for mobile nodes that dealt with location claims (only) and deployment information are not appropriate for mobile WSN, given that position transforms time to time in portable wireless sensor network. And a few alternative approaches for mobile WSN are discussed.

References

[1] Parno, Bryan, Adrian Perrig, and Virgil Gligor. "Distributed detection of node replication attacks in sensor networks." Security and Privacy, 2005 IEEE Symposium on. IEEE, 2005.

[2] Choi, Heesook, Sencun Zhu, and Thomas F. La Porta. "SET: Detecting node clones in sensor networks." Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on. IEEE, 2007.

[3] Brooks, Richard, et al. "On the detection of clones in sensor networks using random key predistribution." IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) 37.6 (2007): 1246-1258.

[4] Zhu, Bo, et al. "Efficient distributed detection of node replication attacks in sensor networks." acsac. IEEE, 2007.

[5] Conti, Mauro, et al. "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks." Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing. ACM, 2007.

[6] Ho, Jun-Won, et al. "Distributed detection of replica node attacks with group deployment knowledge in wireless sensor networks." Ad Hoc Networks 7.8 (2009): 1476-1488.

[7] Baig, Zubair Ahmed, and Asad I. Khan. Distributed denial of service attack detection in wireless sensor networks. Monash University, 2008.

[8] Kalita, Hemanta Kumar, and Avijit Kar. "Wireless sensor network security analysis." International Journal of Next-Generation Networks (IJNGN) 1.1 (2009): 1-10.

[9] Sei, Yuichi, and Shinichi Honiden. "Distributed detection of node replication attacks resilient to many compromised nodes in wireless sensor networks." Proceedings of the 4th Annual International Conference on Wireless Internet. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008.

[10] Bekara, Chakib, and Maryline Laurent-Maknavicius. "A new protocol for securing wireless sensor networks against nodes replication attacks." Wireless and Mobile Computing, Networking and Communications, 2007. WiMOB 2007. Third IEEE International Conference on. IEEE, 2007.

[11] Xing, Kai, et al. "Real-time detection of clone attacks in wireless sensor networks." Distributed Computing Systems, 2008. ICDCS'08. The 28th International Conference on. IEEE, 2008.

[12] Ho, Jun-Won, Matthew Wright, and Sajal K. Das. "Fast Detection of Node Replication Attacks in Mobile Sensor Networks." IEEE ICNP. 2008.

[13] Yu, Chia-Mu, Chun-Shien Lu, and Sy-Yen Kuo. "Mobile sensor network resilient against node replication attacks." Sensor, Mesh and Ad Hoc Communications and Networks, 2008. SECON'08. 5th Annual IEEE Communications Society Conference on. IEEE, 2008.

[14] Yu, Chia-Mu, Chun-Shien Lu, and Sy-Yen Kuo. "Efficient and distributed detection of node replication attacks in mobile sensor networks." Vehicular Technology Conference Fall (VTC 2009-Fall), 2009 IEEE 70th. IEEE, 2009.

[15] Deng, Xiaoming, Yan Xiong, and Depin Chen. "Mobility-assisted detection of the replication attacks in mobile wireless sensor networks." Wireless and Mobile Computing, Networking and Communications (WiMob), 2010 IEEE 6th International Conference on. IEEE, 2010.

[16] Mamun, Mohammad Saiful Islam, and A. F. M. Kabir. "Hierarchical design based intrusion detection system for wireless ad hoc network." arXiv preprint arXiv:1208.3772 (2012).

[17] Manjula, V., and C. Chellappan. "The replication attack in wireless sensor networks: Analysis and defenses." International Conference on Computer Science and Information Technology. Springer, Berlin, Heidelberg, 2011.