International Journal of Research In Science & Engineering
Volume: 3 Issue:1 January 2017

e-ISSN: 2394-8299
p-ISSN: 2394-8280

A Survey on Various Routing Attacks on Wireless Sensor Network

Bhagyashree Shimpi[1], Ms.Sameeksha Shrivastava[2.]

M-Tech Scholar, Sri Aurobindo Institute of Technology,Indore[1]

Assistant Professor, Sri Aurobindo Institute of Technology, Indore2

bhagyashreeshimpi23@gmail.com [1], *sameeksha.shrivastava@sait.ac.in* [2]

ABSTRACT: Security is important factor for several sensor network applications. Wireless sensor Networks (WSN) when deployed in hostile environments as static or mobile, an antagonist will try to physically capture some of the nodes, once 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 form replicas and listen the transmitted messages or adjust the functionality of the network. Identity felony ends up in 2 sorts attack: clone and Sybil. In particularly a catastrophic attack against sensor networks wherever one or more node(s) illegitimately claims an identity as replicas is known as the node replication attack. The replication attack is tremendously injurious to many important functions of the sensor network like routing, resource allocation, mis-behavior detection, etc.

This paper inspect the threat posed by the replication attack and a number of other novel techniques to find and defend against the replication attack, and analyzes their effectiveness in each static and mobile WSN.

KEYWORDS:- Security, Clone, Sybil, node replication attack and static WSN.

INTRODUCTION: A Wireless sensor Network (WSN) may be a assortment of sensors with limited resources that collaborate so as to achieve a common goal. sensor nodes operate in belligerent environments like battle fields and scrutiny zones. due to their operative nature, WSNs ar typically neglected, thus at risk of many forms of novel attacks. The mission-critical nature of sensor network applications implies that any compromise or loss of sensory resource due to a malicious attack launched by the adversary-class will cause significant harm to the whole network. Sensor nodes expanded in a battlefield could have intelligent adversaries operative in their surroundings, intending to subvert harm or hijack messages exchanged within the network. The settlement of a sensor node will result in greater damage to the network. The wealth challenged nature of environments of operation of detector nodes mostly differentiates them from different networks. All security quick fix proposed for sensor networks need to operate with minimal energy usage, while securing the network. The basic security requirements of WSN are availability, confidentiality, integrity and communications [16].

We classify detector network attacks into 3 main categories [7] [8]: Identity Attacks, Routing Attacks &amp; Network Intrusion. Identity attacks intend to steal the integrity of legitimate nodes in operation within the sensor network. The pinpoint attacks ar Sybil attack and Clone (Replication) attack. In a Sybil attack , the WSN is superseding by a malicious node that forges an oversized variety of fake identities so as to di srupt the network's protocols. A node replication attack is an attempt by the adversary to add one or additional nodes to the network that use identical ID as another node within the scenario.

Routing attack will place the rogue nodes on a routing path from a source to the base station could attempt to tamper with or discard legitimate data packets. a number of the routing attacks are sinkhole Attack, False routing data attack, Selective forwarding attack, and Wormholes. The antagonist creates an oversized sphere of influence, which can attract all traffic destined for the base station from nodes which may be many hops away from the compromised node that is known as sinkhole attack. False routing attack means interjecting fake routing control packets into the network. Compromised node may waste to forward or forward selective packets known as as Selective forwarding attack. Within the wormhole attack, 2 or more malicious colluding nodes create higher level virtual tunnel within the network, that is employed to move packets between the tunnel finish points. Network intrusion is an unauthorized access to a system by either an external perpetrator, or by an insider with insignificant privileges.

In this paper we are concentrating on an identity attack known as replication attack wherever one or more nodes illegitimately claim an identity of legitimate node and replicated in whole WSN network as shown Figure 1. Reason for selecting this attack is that it will form the basis of a variety attacks such Sybil attack , routing attacks and link layer attacks, also known as as denial of service attacks that affects availability of network.

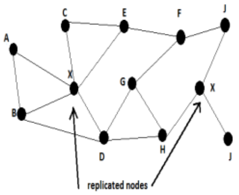

Figure1. Replication Attack

The detection of node replication attacks in a wireless sensor network is so a fundamental problem. some centralized and distributed solutions have recently been proposed. However, these solutions are not gratifying. First, they are energy and memory stringent: a significant drawback for any protocol that is to be used in resource constrained environment like a sensor network. Further, they're susceptible to specific adversary models introduced in this paper.

2. SIGNIFICANCE OF REPLICATION ATTACK AND BACKGROUND

NODE REPLICATION ATTACK

Wireless device network, associate individual 1st physically captures only one or few of appropriate nodes, then clones or replicates them fabricating those replicas having the same identity (ID) with the captured node, and eventually expands a capricious number of clones throughout the network cause of node replication attack are as follows:

It creates an extensive damage to the network as a result of the replicated node also has the same identity because the legitimate member.

It creates various attacks by extracting all the key credentials of the captured node. It debase the monitoring operations by injecting false data. It will cause jamming within the network, rettle the operations within the network and additionally initiates the Denial of Service (DoS) attacks too. It is difficult to tell apart replicated node and therefore authentication is difficult.

A WSN is either stationary or mobile. In static wireless sensor networks (SWSNs), the sensor nodes are stationary or static; that's, the device nodes ar use at random, and once deployment their positions do not diversity. On the other hand, in mobile wireless sensor networks (MWSNs), the sensor nodes will pass on their own, and once readying, showing at completely different|completely different} locations at different times. the benefits include 1) localized detection; 2) efficiency and effectiveness; 3) network-wide synchronization avoidance; and 4) network-wide revocation avoidance.

DETECTION TECHNIQUES

Based on the detection methodologies, classify the clone attack detection.

1.Detection Techniques for Stationary WSNs

2.Detection Techniques for Mobile WSNs

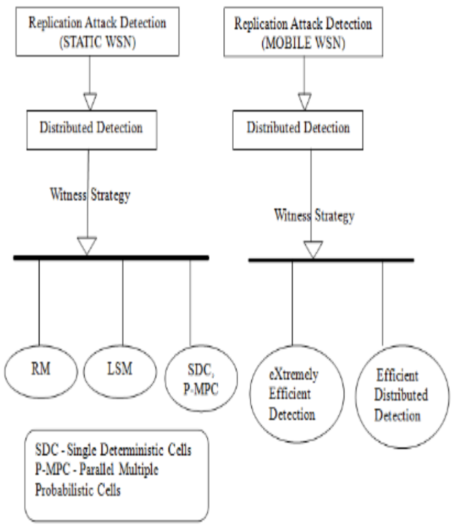
Replication Attack Detection (STATIC WSN)
Replication Attack Detection (MOBILE WSN)
Distributed Detection
Distributed Detection
Witness Strategy
Witness Strategy
RM
LSM
SDC, P-MPC
eXtremely Efficient Detection
Efficient Distributed Detection
SDC - Single Deterministic Cells
P-MPC - Parallel Multiple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

Fig.2 Steps of replication attack detection

Witness-Finding Strategy:- Node broadcast its location claim to its neighbours, shares a nodes location claims with a limited set of chosen witness nodes. Checking whether or not there are the same ID's used at different location to detect the replicas. Static networks trust on the witness-finding technique, that can not be applied to mobile networks.

1.DETECTION TECHNIQUES FOR STATIONARY WNS’s

The detection of node replication attack in static WSNs that ar categorised in the main into 2 sorts as centralized and distributed techniques.

(A) Centralized Techniques: In centralized techniques base station is considered 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 usage exceeds a threshold can be judged to be cloned. within 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 base station public key; this encrypted data structure 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 sub tree. each subgroup leader collects member information and forwards it to the root of the sub tree. The crossing operation is performed on each root of the sub tree to detect replicated nodes. If the crossing of all subsets of a sub tree is vacant, there aren't any clone nodes during this sub tree. in the end, each root forwards its report to the base 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 bs 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 central authority exists, and special detection mechanism known as claimer-reporter-witness is provided within which the detection is performed by locally distributed node sending the location claim to not the bottom station (sink) however to a randomly selected node known as witness node.

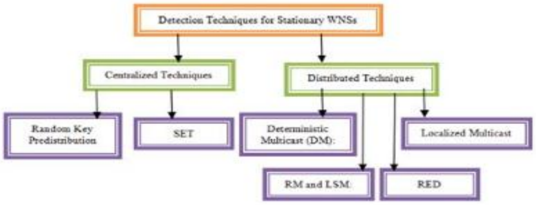
Detection Techniques for Stationary WNSs
Centralized Techniques
Distributed Techniques
Random Key Predistribution
SET
Deterministic Multicast (DM)
Localized Multicast
RM and LSM
RED

Fig:.3 Detection techniques for stationary WNSs

(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 employs a 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 the 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 path (from claiming node to the witness destination) forwards the message to its neighbor nearest to the destination. Hence, the replicated nodes are 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.

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, AOMDV, DSDV and PEGASIS protocols to investigate that one style of protocol provides higher performance.

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 trust values:

1.If the packets are correctly transmitted 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 + (correctly transmitted packets / 10);

2.If the packets are dropped/delayed :

(a) The number of dropped or delayed packets is between 1 and 10,and then trust value of that particular node is decremented by one.

Updated trust value = old trust value – 1;

(b) The number of dropped or delayed packets are greater than 10, then trust value of that particular node will be,

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

1. If the trust value of particular node is negative, then print “Invalid node”.

[C] Isolating the Packet drop node from the network:

1. If (Updated 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.

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 bystander based strategy of distributed approaches, randomness 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 compromised node or cloned node then detection of replication attack is uncertain. There is also trade-off between communication cost overhead and detection rate.

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 be 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, since location changes time to time in mobile wireless sensor network. And a few alternative approaches for mobile WSN are discussed.

REFERENCES

[1]. Parno B, Perrig A, Gligor V. "Distributed Detection of Node Replication Attacks in Sensor Networks" In: Proceedings of the IEEE Symposium on Security and Privacy; 2005. p. 49 – 63.

[2]. Choi H, Zhu S, La Porta TF. "SET: Detecting node clones in sensor networks" In: Third International Conference on Security and Privacy in Communications Networks and the Workshops (SecureComm 2007); 2007. p. 341–350

[3]. Brooks R, Govindaraju PY, Pirretti M, Vijaykrishnan N, Kandemir MT. "On the Detection of Clones in Sensor Networks Using Random Key Predistribution" IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews. 2007;37(6):1246–1258.

[4]. Zhu B, Addada VGK, Setia S, Jajodia S, Roy S. "Efficient Distributed Detection of Node Replication Attacks in Sensor Networks" In: Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007); 2007. p. 257–267

[5]. M. Conti, R. Di Pietro, L.V. Mancini, and A. Mei "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks" In ACM MobiHoc, pages 80–89, 2007

[6]. Jun –Won Ho, Donggang Liu, Mathhew wright, Sajal K.Das , " Distributed detection of replica node attacks with group deployment knowledge in wireless sensor networks", Ad Hoc Networks, 2009, 1476 – 1488

[7]. Zubair A. Baig "Distributed Denial of Service Attack Detection in Wireless Sensor Networks", 2008, thesis.

[8]. Hemanta Kumar Kalita and Avijit Kar, "Wireless Sensor Network Security Analysis, International Jo urnal of Next-Generation Networks (IJNGN),Vol.1, No.1, December 2009.

[9]. Yuichi Sei , Shinichi Honiden , "Distributed Detection of Node Replication Attacks resilient to Many Compromised Nodes in Wireless Sensor Networks", 2008 ICST

[10]. Bekara, M. Laurent-Maknavicius. "A new protocol for securing wireless sensor networks against no des replication attacks", In Proceedings of the 3rd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2007.

[11]. K. Xing, F. Liu, X. Cheng, D. H.C. Du. "Real-time detection of clone attacks in wireless sensor net works", In Proceedings of the 28th International Conference on Distributed Computing Systems (ICDCS) , 2008.

[12]. Jun-won ho, Matthew wright, and Sajal k. Das, "fast detection of node replication attacks in mobile sensor networks" , in IEEE ICNP 2008 (poster)

[13]. Chia-Mu, Y., Chun-Shien, Lu., and Sy-Yen, K. 2008. Mobile Sensor Network Resilient Against No de Replication Attacks. SECON '08. 5th Annual IEEE Communications Society Conference on , vol., no., pp.597-599. (poster)

[14]. Chia-Mu Yu, Chun-Shien Lu and Sy-Yen Kuo, "Efficient distributed and detection of node replicati on attacks in mobile sensor networks" IEEE 2009.

[15]. Xiaoming Deng, Yan Xiong, and Depin Chen , "Mobility-assisted Detection of the Replication Atta cks in Mobile Wireless Sensor Networks" 2010 IEEE 6th International Conference on Wireless and Mobi le Computing, Networking and Communications.

[16]. Mohammad Saiful Islam Mamun and A.F.M. Sultanul Kabir, "Hierarchical Design Based Intrusion Detection System For Wireless Ad Hoc Sensor Network" International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3, July 2010

[17]. V.Manjula and Dr.C.Chellappan, "The Replication Attack in wireless Sensor Networks: Analysis & Defenses" , CCIST 2011, Communications in Computer and Information Science, Volume 132, Advance s in Networks and Communications, Part II, Pages 169-178, book chapter, Springer –Verlog.