International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

A Review on Various Routing Attacks on Wireless Sensor Network

Aruna Rantore[1], Kapil Vyas[2]

[1]B, M College Indore, India

[2]Assistant Professor, B, M College Indore, India

Abstract: ***Security is relevant for many sensor network applications. Wireless Sensor Networks (WSN) is often deployed in hostile environments as static or mobile, where an antagonist can physically capture some of the nodes, once a node is captured, antagonist collects all the credentials like keys and identity etc. the attacker can re-program it and repeat the node in order to eavesdrop the transmitted messages or adjustment the functionality of the network. Identity burglary leads to two types attack: clone and Sybil. In particularly a catastrophic attack against sensor networks where one or more node(s) illegitimately claims an identity as replicas is known as the node replication attack. The replication attack can be enormously injurious to many important functions of the sensor network such as routing, resource allocation, mis-behavior detection, etc. This paper inspect the threat posed by the replication attack and several novel techniques to detect and defend against the replication attack, and analyzes their effectiveness in both static and mobile WSN.***

Keywords: Security, Clone, Sybil, node replication attack and static WSN

1. Introduction

A Wireless Sensor Network (WSN) is a collection of sensors with limited resources that collaborate in order to achieve a common goal. Sensor nodes operate in belligerent environments such as battle fields and scrutiny zones. Due to their operating nature, WSNs are often neglected, hence prone to several kinds 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 can cause significant damage to the entire network. Sensor nodes expanded in a battlefield may have intelligent adversaries operating in their surroundings, intending to subvert damage or hijack messages exchanged in the network. The settlement of a sensor node can lead to greater damage to the network. The wealth challenged nature of environments of operation of sensor nodes largely differentiates them from other networks. All security quick fix proposed for sensor networks need to operate with minimal energy usage, whilst securing the network. So the basic security requirements of WSN are availability, confidentiality, integrity and communications [16].

We classify sensor network attacks into three main categories [7] [8]: Identity Attacks, Routing Attacks & Network Intrusion. Identity attacks intend to steal the integrity of legitimate nodes operating in the sensor network. The pinpoint attacks are Sybil attack and Clone (Replication) attack. In a Sybil attack, the WSN is superseding by a malicious node which forges a large number of fake identities in order to disrupt the network's protocols. A node replication attack is an attempt by the adversary to add one or more nodes to the network that use the same ID as another node in the scenario.

Routing attack intend to place the Rogue nodes on a routing path from a source to the base station may attempt to tamper with or discard legitimate data packets. Some of the routing attacks are Sinkhole Attack, False routing information attack, Selective forwarding attack, and Wormholes. The antagonist creates a large sphere of influence, which will attract all traffic destined for the base station from nodes which may be several hops away from the compromised node which is known as sinkhole attack. False routing attack means that interjecting fake routing control packets into the network. Compromised node may waste to forward or forward selective packets called as Selective forwarding attack. In the wormhole attack, two or more malicious colluding nodes create higher level virtual tunnel in the network, which is hired to transport packets between the tunnel end 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 called replication attack where one or more nodes illegitimately claim an identity of legitimate node and replicated in whole WSN network as shown Figure 1. Reason for choosing this attack is that it can form the basis of a variety attacks such Sybil attack, routing attacks and link layer attacks, also called as denial of service attacks which affects availability of network.

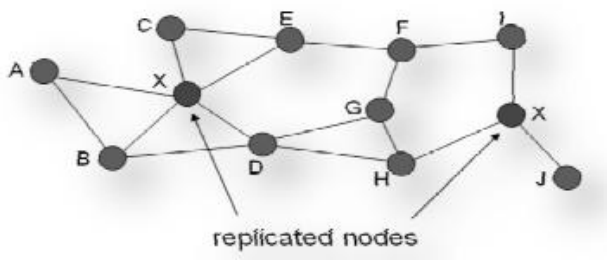

Figure 1: Replication Attack

The detection of node replication attacks in a wireless sensor network is therefore a fundamental problem. A few

centralized and distributed solutions have recently been proposed. However, these solutions are not gratifying. First, they are energy and memory stringent: A serious drawback for any protocol that is to be used in resource constrained environment such as a sensor network. Further, they are susceptible to specific adversary models introduced in this paper.

2. Significance of Replication Attack and Background

Node Replication Attack

Wireless sensor network, an adversary first 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 finally expands a capricious number of clones throughout the network cause of node replication attack are as follows:

- It creates an extensive harm to the network because the replicated node also has the same identity as the legitimate member.
- It creates assorted attacks by extracting all the secret credentials of the captured node.
- It debase the monitoring operations by injecting false data.
- It can cause jamming in the network, rettle the operations in the network and also initiates the Denial of Service (DoS) attacks too.
- It is difficult to distinguish replicated node and hence authentication is difficult.

A WSN can be either stationary or mobile. In static wireless sensor networks (SWSNs), the sensor nodes are stationary or static; that is, the sensor nodes are use randomly, and after deployment their positions do not diversity. On the other hand, in mobile wireless sensor networks (MWSNs), the sensor nodes can move on their own, and after deployment, appearing at different locations at different times. The advantages 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.

Detection Techniques for Stationary WSNs

Detection Techniques for Mobile WSNs

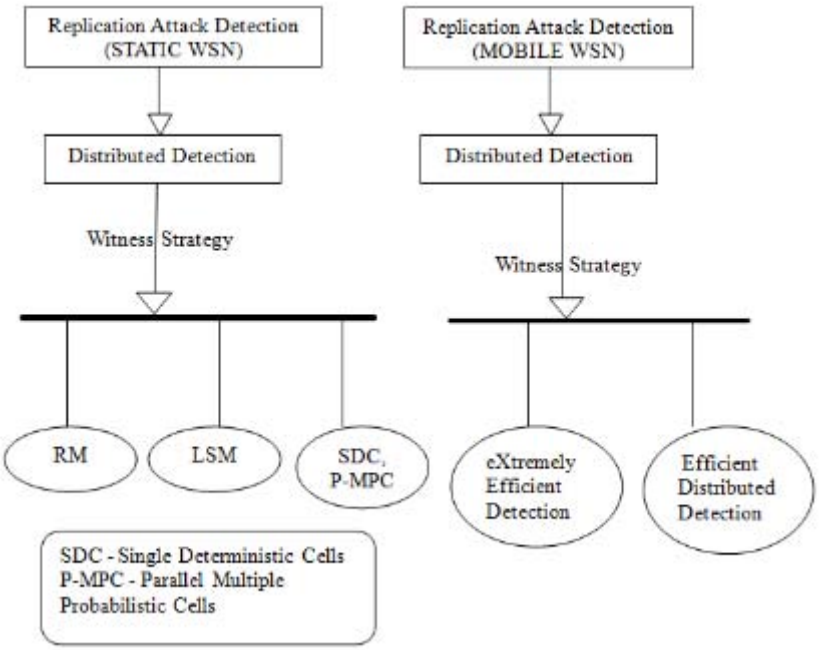

Figure 3: Steps of replication attack detection

Witness-Finding Strategy:- Node broadcast its location claim to its neighbors, shares a nodes location claims with a limited subset of chosen witness nodes. Checking whether there are the same ID's used at different location to detect the replicas. Static networks trust on the witness-finding method, which cannot be applied to mobile networks.

3. Detection Techniques for Stationary WNS's

The detection of node replication attack in static WSNs which are categorized mainly into two types as centralized and distributed techniques.

Centralized Techniques: In centralized techniques base station is considered to be a powerful central which is responsible for information convergence and decision making. During the detection growth every node in the network sends its location allegation (ID, Location Info) to base station (sink node) through its neighboring nodes. Upon receiving the entire location allegation, the base station checks the node Ids along their location, and if it finds two locations with the same ID, it hikes a clone node.

Random Key Pre distribution:[1] The basic idea is that the keys employed according to 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. In the protocol, counting Blossom filters is used to collect key

usage statistics. Each node makes a counting Blossom filter of the keys it uses to communicate with neighboring 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 each 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. Each node decrypts base stations blossom filter removes cloned keys from its keying, and terminates connections using cloned keys.

SET:[3] The network is randomly divided into exclusive subgroup. Each of the subsets has a subspace leader, and members are one hop away from their subgroup leader. Multiple roots are randomly decided 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 bare, there are no clone nodes in this sub tree. In the final stage, every root forwards its report to the base station (BS). The base station detects the clone nodes by computing the crossing of any two received sub trees. SET identify clone nodes by sending node information to the BS from subset leader to the root node of a randomly constructed sub tree and then to the BS.

Distributed Techniques: Distributed techniques consist no central authority exists, and special detection mechanism called claimer-reporter-witness is provided in which the detection is performed by locally distributed node sending the location claim not to the base station (sink) but to a randomly selected node called witness node.

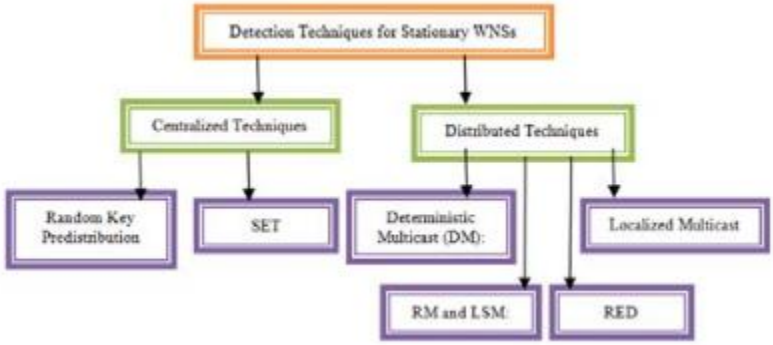

Figure 4: Detection techniques for stationary WNSs

1. Deterministic Multicast (DM):[2] DM protocol is a claimer-reporter-witness framework. The claimer is a node which locally broadcasts its location claim to its neighbors, each neighbor dollop as a reporter, and employs a function to map the claim ID to a witness. Then the neighbor forwards the claims to the bystander, which will receive two different location claims for the same node ID if the antagonist has replicated a node. One problem can occur that the adversary can also employ the function to know about the witness for a given claim ID, and may locate and compromise the witness node before the adversary inserts the replicas into the WSN so as to evade the detection.

2. RED:[5] Randomized, Efficient, and Distributed protocol called RED, for the detection of node replication attack. It is assassinate at fixed intervals of time and consists in two steps. In first step, a random value, randomly, is shared between all the nodes through base station. The next step is called detection phase. In this phase, each node broadcasts its claim (ID and location) to its neighboring nodes. Each neighbour node that hears a claim sends (with probability p) this claim to a set of pseudo randomly selected network locations. The pseudo random function is taking as an input ID, random number. Every node in the path (from claiming node to the witness destination) forwards the message to its neighbor nearest to the destination. Hence, the replicated nodes will be detected in each detection step. When next time the RED executes, the witness nodes will be differ since the random value which is broadcasted by the BS is changed.

4. Objective

An objective of this thesis work is as follow:

- The study focus on analysis of WSN Routing Protocol.
- Prepare the Wireless Sensor Network (WSN) scenario with simulation time of 100sec with 10 nodes, 15 nodes and 20 nodes.
- Analyzing the effects of residual energy, throughput, normalized routing load and network lifetime in WSN scenario with different environment.
- Analyzing the results of AODV, AOMDV, DSDV and PEGASIS protocols to analyze which one type of protocol gives better performance.

5. Proposed Algorithm

The proposed algorithm is based on the trust values of individual nodes. All the nodes of wireless ad-hoc network have a specific trust value. The algorithm encompasses the following steps:

[A] Initialization

1) Trust values of all the participating nodes are 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);

3) If the trust value of particular node is negative, then print "Invalid node".

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

4) If (Updated trust value < Threshold trust value)
Then the particular node is treated as malicious node (Black hole node)

5) 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 more advantages than centralized approaches since single point failure. In bystander based strategy of distributed approaches, randomness introduced in choosing witnesses at various levels like whole network and limited 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 may be trade-off between communication cost overhead and detection rate. All the approaches dealt with static WSN. With the deployment knowledge (like order, neighborhoods, and group members with locations) all the nodes in the network should know highest deployed generation which impractical and cannot move join other groups since neighbors or fingerprints vary. Some WSN application requires mobile nodes. The entire access become complex when considering for mobile nodes which dealt with location claims(only) and Deployment knowledge are not suitable for mobile WSN, since location changes time to time in mobile wireless sensor network. And some other approaches for mobile WSN have been 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 Journal 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 nodes 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 networks", 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 Node 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 replication attacks in mobile sensor networks" IEEE 2009.

[15] Xiaoming Deng, Yan Xiong, and Depin Chen , "Mobility-assisted Detection of the Replication Attacks in Mobile Wireless Sensor Networks" 2010 IEEE 6th

International Conference on Wireless and Mobile 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, Advances in Networks and Communications, Part II, Pages 169-178, book chapter, Springer –Verlog.