A Review on Various Routing Attacks on Wireless Sensor Network

*** Bhagyashri N. Jadhav**
**** Hemant Kumar Gupta**

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 preserve adjacent to the replication attack, and considers their effectiveness in each static and mobile WSN

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

* Bhagyashri N. Jadhav, Student, M. Tech, Department of Computer Science, Lakshmi Narain College of Technology and Science (RIT), Indore, bhagyashrij14@gmail.com
** Hemant Kumar Gupta, Assistant Professor, Department of Computer Science Lakshmi Narain College of Technology and Science (RIT), Indore

I. 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 are typically neglected, thus at risk of many forms of novel attacks. The mission-critical nature of sensor network applications implies that any cooperation or defeat of sensory reserve 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 ease of use, discretion, reliability and messages [16].

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. We classify detector network attacks into 3 main categories [7] [8]: Identity Attacks, Routing Attacks & Network Intrusion. Identity attacks intend to steal the integrity of legitimate nodes in operation within 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 that forges an oversized variety of fake identities so as to disrupt 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.

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 false direction-finding organize packets into the system. concession 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 entrance to a organism by each an exterior perpetrator, or by an insider with insignificant privilege.

In this paper we are focuses on an individuality attack well-known as replication attack wherever one or more nodes illegitimately maintain an individuality of reasonable node and replicated in complete 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 replica attacks that affects availability of network.

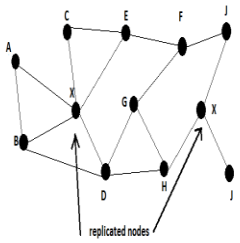

Figure 1. Replication Attack

The recognition of node replication attacks in a wireless antenna network is so a fundamental problem. some centralized and circulated explanations have only just been recommend. though, 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. 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, 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 from set leader to the root node of a randomly created sub tree.

II. PROPOSED METHODOLOGY

Replica detection is a widely accepted approach to handle node replication attack in sensor networks. An efficient node replica detection mechanism should not only detect a replica but also optimize the overall network performance. Further, the replica detection mechanism should emphasize not only on higher detection probability but also on lower communication and storage overhead. In this thesis, we have studied the behavior of node replication attack and identified the possible ways an original node can be distinguished from its replica. A WSN is either stationary or mobile. In static wireless sensor networks, the sensor nodes are stationary or static; that's, the device nodes are use at random, and once deployment their positions do not diversity. On the further hand over, in portable wireless sensor networks, 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) effectiveness and efficiency; 3system-wide organization avoidance; and 4) network-wide revocation avoidance.

III. DETECTION METHODS

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

1. Detection Techniques for Stationary WSNs

2. Detection Techniques for Mobile WSNs

IV. 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 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, 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 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.