International Journal of Future Generation Communication and Networking
Vol. 13, No. 3s, (2020), pp. 1546–1548

A Secure Model for Detecting Origin Forgery and Packet Drop Attacks in Wireless Network

Pranali Salunkhe, Sandesh Thorat , Prateek Parihar, P.T. Suradkar

BE Student, NBNSSOE
*Computer Department
** NBN Sinhgad School Of Engineering*

Abstract

Wireless sensor network uses the data collected from various data nodes for the decision-making process. But advisory nodes tend to compromise and temper with the data and because of that data gets altered. Provenance is used for verifying the data but some problems may arise while doing so like bandwidth consumption and space complexity.

I. INTRODUCTION

T he packets delivery ratio gets affected by the packet loss. This packet loss is caused by number of factors like degradation of signal. packet degradation is caused by path fading measures have to be taken in order to secure transmission. There is a special case that we need to keep in mind in which intruder captures this packet for that the technique is been extended for packet loss attacks.

In this the main goal is to make use of bloom filter for data encoding, this bloom filter stores prominence for securely transmitting the data. The base station which is the Main node checks this information.

II. FINDINGS & IDEA

1) S. Roy, M. Conti, S. Setia, and S. Jajodia[1], In a wireless sensor network, in-network data aggregation substantially reduces the communication amount and consumption of energy. Recently, the researcher's has proposed a robust aggregation framework called synopsis diffusion which is used for combing multipath routing schemes with duplicating sensitive algorithms so that accurate aggregates can be computed. Even with message losses resulting node and transmission failures. This aggregation framework does not solve the problem of false sub aggregate values captured by compromised nodes resulting in large errors in the aggregate computed at the base station, which is the root node. This is an important aspect since sensor networks are highly vulnerable to node compromised data due to the unattended nature of sensor nodes and the lack of tamper resistant hardware. T. Wolf [2], Capabilities-based networks plays an important role in a fundamental shift in the security design of network architectures. Instead of allowing the transmission of packets from any source to destination, routers denies forwarding packets. For a successful transmission, packets have to positively identify itself and its permission to the router. The analysis of the data paths. Data structure that et.al propose shows that 128 bits can be sufficient to decrease the probability of unauthorized traffic going its destination to a fraction of a percent. S. Marti, T. J. Giuli, K. Lai, and M. Baker [3] et.al tells about two techniques that can improve throughput in an ad hoc network in the nodes that agree to forward packets but fail to do so. To conquer this problem, we propose categorizing nodes based on dynamically measured behavior of them. Technique makes use of a watchdog that identifies these misbehaving nodes and a path that

ISSN: 2233-7857 IJFGCN

helps routing protocols to avoid these nodes. By the use of these simulation technique we evaluate watchdog and path rater using packet throughput, percentage of overhead routing, and the accuracy of misbehaving node detection.

III. IMPLIMENTATION

1:Data Packet Representation: To detect packet loss and ensure secured transmission of packets we use provenience inn which each packet header has unique sequence number . Each next node has last ones sequence number starting from source node. Each intermediate node have his own unique sequence number , previous packets sequenced number , data value and provenance.

2. **Provenance Encoding** Secure encoding technique is very good operation technique and to detect data intigrity. It uses a distributed mechanism to encode Provenance at the nodes and a provenance decoding algorithm so it can decode it at the base station. It uses in-packet BF . Each packet has a uspecific sequence number, data number, and an bloom filter which is used for holding the provenance. The main function is on transfering psignificance to the Base station. The provenance record of a node includes nodeID and acknowledgement of the last obtained packet in the following flow.

3. **Provenance Decoding** security is an important aspect at base station . Base station is a platform also called as root node where after transfer of packets from source node to middle way node data packets end up . This base station verifies provenance and updates the important parts . now here the system sees all the functions , Verification and collection is the main function of base station .

4.**Detecting Packet Drop** As the result of the followed up process and along with help of various MAC addresses , the software can detect the manipulations at sensor nodes , The proposed system is capable enough of finding out the hackers and lost packets in depth.

Together when seen on a large scale the system looks like a forensic set up. Acknowledgements generated during transmission are used for detecting these drop attacks and malicious nodes .

IV RESULT

Here we use Ns2 netwrok and seen a hilarious performance . the systems were showing more reliability . Along with that the chances of attacks were reduced by 97% . The data that was transmitted from source node to the destination node was unchanged and raw , Which indicated that the data is fully true and trust worthy.

Ssp , MMP and the provinence technique was very reliable . Comparing all three our software showed full trustworthiness. The provenance Length in SSP and MP becomes larger linearly with the linear length. The BF size grows allot with the expected quantity of elements to be inserted, the increasing rate is not linear. In following scheme the data transmission only needed 30 bytes of total data and it can handle uptoo 35 hopps.

. The process undergoes the following phases:

We consider the problem of secure provenance transfer in wsn.

- The Proces of implementation of an in-packt BF provenance encoding system.
- technique and uses of decoding and verification.
- Detection of malicious activities through design mechanism.
- Detailed security analysis through this system.
- The fast schemes and Bloom filters are fixed and speed is increased

ISSN: 2233-7857 IJFGCN

 Bloom filter ensures good usage of required bandwidth .
 Confidentiality claim : - BF is device that is more trust worthy then any other software
 Claim For Integrity: - A single attacker or a multiple user platform can be detected through Mac Addresses.

v. CONCLUSION

As the major concern was to see how the hackers are still capable of performing the false activities , the biggest question that was raised is " how the attacks takes place and what are the preventions .
Here after all the experimentations the systems helped in concluding the idea of stopping the packet drop attacks . This Way ensured confidentiality, integrity and freshness of the provenance data. Experimental techniques are used for analyzing the data , that was collected from the resources . resultant scheme is scalable and lightweight.

Refrences

[1] E. Bertino, and H limo, "Provenance-Based Trustworthiness Assessment in Sensor Networks," Proc. eithth Int'l Workshop DBMS for Sensor WSN, pp. 2-7, 2010.
[2] I. Fostered, J. Vockler, "Chimera: A Virtual Data System for Representing, Querying, and Automating Data
[3] Derivation," Proc234. Conf9. Scientific and Statistical Dbms,pp. 37-4634, 2002.
[4] K. Munaswamy-, D. Hollund, U. Braun, and M. Seltzer, "Provenance-Aware Storage systems," Proc. USENIX Ann. Technical Conf., pp. 4-4, 2006. Y. Simmhan, B. Pranalie, and P. Gannon, "A Survey of Data Provenance in E-Science," ACMSIGMOD Record, vol. 34, pp. 31-36, 2005
[5] Rh. Hasan, R. Sion, and M. Winslett, "The Case of the Fake Picasso: Preventing History Forgery with Secure Provenance," Proc. Seventh Conf. File and Storage Technologies (FAST), pp. 1-14, 2009
[6] A. Rama h. chandran, K. Bhand, M. Tariq, , "Packets with Provenance," Tech. conclusion GT-CS-08-02, Georgia Tech, 2008.
[7] W. Zhoux, Q. wen, A. Narayan, A. burmingam donald, B. Loo, and M.c. Sherr, "Secure Network Provenance," Proc. ACMSOSP, pp. 295-310, 2011.
8] W. Zhounk, M.c, Sherr, T. Taco, X. Li, B. Loobo, and Y. Mao, "Efficient Querying and Maintenance of Network Provenance at Internet- Scale," Proc. ACM.
[9] N. Vijayakumar and B. Plale, "Towards Low Overhead Provenance Tracking in Near Real-Time Stream Filtering," Proc. Int'l Conf. Provenance and Annotation of Data (IPAW), pp. 46-54, 2006.
[10] A. Salim, T. Suleman, and jubaan Kesari, "Preserving Integrity and Conf. of a Directed Acyclic Graph Model of Provenance," . Security and Privacy, pp. 3121-3138, 20910.

ISSN: 2233-7857 IJFGCN