AN EFFICIENT DETECTION OF FORGERY AND PACKET DROP ATTACKS IN WIRELESS SENSOR NETWORKS THROUGH IN-NETWORK AGGREGATION SCHEME

M.Tharani,
PG Student,
Sasurie Academy of Engineering,
Coimbatore, India.

K.Sivachandran,
Assistant Professor,
Sasurie Academy of Engineering,
Coimbatore,India.

T.Lakshmana kumar,
Assistant Professor,
Sasurie Academy of Engineering,
Coimbatore,India.

Abstract: In large scale sensor networks contain various applications and domains. The data composed from wireless sensor network are used under making decisions in critical infrastructures. Data's are generated from multiple sources those are transmitted through intermediate processing nodes. The aggregation function should be performed by the intermediate nodes. An attacker compromise those type of intermediate nodes by introducing additional attacking nodes in the network or compromising the existing nodes in the network. So achieving the high data trustworthiness is critical for correct decision-making. The provenance management challenges in sensor networks are consumption of low energy and low bandwidth consumption. This survey introduces a new lightweight scheme in order to securely transmit sensor data with provenance. The in-packet Bloom filters techniques used to encode provenance with the sensor data. This mechanism initially performs provenance at the source then perform restoration of the data at the destination. The provenance scheme functionality used to detect packet drop attacks organized by malicious intermediate data forwarding nodes. This survey describes the effectiveness and efficiency of the Light weight secure provenance scheme in detecting packet forgery and packet loss attacks through In Network Aggregation scheme. This scheme reduces the energy cost of processing in wireless sensor networks also there is *no currently* solution providing *both* integrity and confidentiality. Moreover, existing solutions allow only limited data transfer from 15MB to 25MB.So they have limited applicability to certain types of application. Recently, research has focused on *secure exact* in-network aggregation. Secure Exact In Network Aggregation use multi path approach. Secure Exact In Network Aggregation increase the data rate of data transfer up to 2GB from 25 MB based on the tree based approach .This approach perform aggregation by constructing an multipath, which could be a minimum spanning tree, rooted at sink and source nodes are considered as leaves. Each node has a parent node to forward its data. Flow of data starts from leaves nodes up to the sink and therein the aggregation done by multi path start from failed nodes rather at source node.

Keywords: Provenance, security, sensor networks, Packet drop attack, Wireless Sensor Networks, Provenance attack.

I.INTRODUCTION

Sensor networks are used in various areas like such as cyber physical infrastructure systems, environmental weather monitoring, power grids, etc. Data are originated from a huge number of sensor node sources and they are processed at intermediate hops at in networks. These data's finally going to a base station (BS) which performs decision-making about where to go next. The uniformity of data sources creates assurance of the trustworthiness of data. This type of trustworthy information is considered in the decision making process at the base station. The data trustworthiness is assured by data provenance scheme. This is an effective method since it summarizes the history of ownership on the data and the list of actions performed on those information.

The big advantage of this provenance scheme is detecting packet loss attacks organized by malicious/compromised sensor nodes. The major disadvantage of this scheme is the use of untrustworthy data at the nodes may create the catastrophic failures (e.g., SCADA systems). Although provenance modeling, collection, and querying have been used extensively in workflows [1] and curated databases [2], provenance at sensor networks has not been fully addressed.

In packet Boom Filter (iBF) [3]

This is a distributed mechanism in order to encode provenance at the nodes and it will work as centralized algorithm to decode it at the BS. The technical core of this survey is the notion of (iBF) [3]. In this packet consists of a unique sequence number, data value, and an iBF which contains the provenance. The focus of this scheme is a

securely transmitting provenance with the data to the BS. In this aggregation framework, securing the data values is an important factor,. The secure provenance technique can be used to obtain a complete solution that provides security for data, provenance and data-provenance binding.

The three Security Objectives in sensor networks is a confidentiality, Integrity and freshness.

Confidentiality : An attacker by analyzing the contents of a packet cannot gain any knowledge about data provenance. Only authorized users (e.g., the BS) can process the information and check the integrity of provenance.

Integrity: An attacker, acting individually or combining with others in a group, cannot add or remove non-colluding nodes. Also the attacker cannot add any data from the malicious user to the orginal data.

Freshness: An attacker cannot replay the captured data from the original user and ensure the provenance detected by the BS. It is also important to provide a coupling between data and provenance i.e. Data-Provenance Binding, so the attacker cannot successfully drop or alter the legitimate/valid data while containing the provenance with the data, or swapping the provenance of two packets

Detecting Packet Drop Attacks

Provenance encoding could be used for a packet acknowledgement. By using this sensor can transmit more meta-data. For an any individual data packet, the provenance record generated by a node will now consist of the node ID and an acknowledgement in the form of a sequence number of the lastly seen (processed/forwarded) packet belonging to that data flow. If the intermediate packet could be drop by the attacker means some nodes on the path do not receive that packet. Hence, during the next round of packet transmission the mismatch between the acknowledgements should be generated from different nodes on the path. This factor could be to detect the packet drop attack and to localize the malicious node.

II.LITERATURE SURVEY

[2]In 2006 K. Muniswamy-Reddy et al, propose "Provenance-Aware Storage systems," .This survey states that in a multi-hop sensor network by using the data provenance scheme the BS can trace the source and forwarding path of an individual data packet. For each packet Provenance must be recorded but there is an important challenge arises due to the heavy storage, energy and bandwidth conditions of sensor nodes. So, it is necessary to provide a light-weight provenance socheme with low overhead.

Disadvantage

- Sensors often operate in a un trusted environment, so there may chance of attacks.
- The necessary to address security requirements such as confidentiality, integrity and freshness of provenance should be increased.

[4]In 2005 R. Hasan et al proposes "threat model for wireless sensor networks". The assumption about the BS is it should be a trusted one, but if any other arbitrary node may be attacked means the also be changed to malicious. An attacker can eavesdrop and perform traffic analysis anywhere on the path. In addition to this he/she is able to organize a few malicious nodes, as well as compromise/attack a few legitimate nodes by capturing them and physically overwriting their memory. If an attacker compromises a node means it can extract all key materials, data, and codes stored on that node. The adversary can drop, inject or alter packets on the links which are under the control of attacker. Also the attacker can create the denial of service attacks such as the complete removal of provenance. If a data packet does not contain no provenance records means it considered as highly suspicious data and hence generate an alarm/signal at the BS about this malicious packet arrival. To overcome this type of detection the attacker attempts to misrepresent the data provenance

[5] In 2012 S. Roy et al propose "Secure Data Aggregation in Wireless Sensor Networks," .This work deals with attacks against the synopsis diffusion. This aggregation work presents a lightweight verification algorithm to make verification at the BS. The several synopses generated should be verified independently by the verification protocol at three phases. The phases are query dissemination phase, aggregation phase and the verification phase. In the first phase called query dissemination phase, the BS broadcasts the aggregation name to compute a random seed. In second phase called the aggregation phase, each node computes a sub aggregate value based on the local value and the synopses of its children. The node also randomly selects a set of MACs .From the selected MACs check whether it should be the received ones from its children. Finally, in the third phase called verification phase, the BS computes the final synopses using the messages from its child nodes and verifies the received MACs.

Disadvantage

- Employs separate transmission channels for data and provenance [6] but the provenance only requires a single channel for both.
- Furthermore, traditional provenance security solutions use intensively cryptography and digital signatures [4], and they employ append-based data structures to store provenance, leading to prohibitive cost and time.

[7] In 2008 A. Ramachandran et al proposed "Packets with Provenance" .This scheme catches provenance for network packets in form of per packet tags. The captured information stores a history of all nodes and processes that packet and manipulates those packets. However, this scheme assures a trusted environment which is not practical in sensor networks.

[8] In 2010 W. Zhou et.al proposes "Querying and Maintenance of Network Provenance at Internet- Scale" which describes the history and sub part of the network state. This result came from the execution of a distributed protocol. The disadvantage of this system is also does not address security concerns and is specific to some network use cases.

[9] In 2011W. Zhou, et.al, proposes a "Secure Network Provenance," .This extends network provenance up to the adversarial environments. Even though all of these systems are general purpose network provenance systems but they are not optimized for the resource constrained sensor networks.

[10] In 2010 A. Syalim et al propose a "Preserving Integrity and Confidentiality of a Directed Acyclic Graph Model of Provenance," .The chain model of provenance ensure integrity(no one can change the data other than the original user) and confidentiality(no one can see the data other than original user)through encryption, checksum and incremental chained signature mechanism. Syalim et al. extend this method by applying digital signatures. This signature applied to a DAG model of provenance.

Disadvantage:-

- These generic solutions are not aware of the sensor network specific assumptions, constraints, etc.
- Since provenance tends to grow very fast, transmission of a large amount of provenance information along with data will incur significant bandwidth overhead, hence low efficiency and scalability.

[11] In 2006 N. Vijaya kumar et al proposes "Towards Low Overhead Provenance Tracking in Near Real-Time Stream Filtering,". This system is an application specific system for near-real time provenance collection in data streams. Nevertheless, this system traces the source of a stream long after the process has completed.

[12] In 2010 Chong et al proposes" Self-Identifying Sensor Data". This scheme embeds the provenance of data source within the data. While it reflects the issues related to the confidentiality, Integrity and efficiency but it is not considered as a security mechanism. Also it does not deal with malicious attacks. However practical issues like scalability, data degradation have not been well addressed. In networking applications Bloom Filters are commonly used. In Packet Bloom Filters have only recently gained more attention being utilized in applications such as credential based data path security [13], IP trace back [14], source routing and multicast [15], [16], etc. The basic idea in these works is to encode the link identifiers constituent to the packet routing path into an In Packet Bloom Filter.

Disadvantage

- The encryption of the whole path is performed by the data source and the intermediate routers check their membership in the In Packet Bloom Filter and forward the packet further based on the decision. This approach is infeasible for sensor networks where the paths may change due to dynamic nature.
- An intermediate router only checks its own membership which may create several integrity attacks such as all-one attack, random bit flips, etc.

III.EXISTING SYSTEM

The goal is to design a provenance encoding and decoding mechanism which satisfies security and performance needs. It proposes a provenance encoding strategy in that each node on the path of a data packet securely embeds provenance information within a Bloom filter (BF) should be transmitted along with the data. While receiving the packet the Base Station extracts and verifies the provenance information. The extension of the provenance encoding scheme allows the BS to detect packet drop attack organized by a malicious node. The features are

- Formulate the problem of secure provenance transmission in sensor networks, and identify the challenges specific to this context.
- Design an effective technique for provenance decoding and verification at the base station.
- Extend the secure provenance encoding scheme and devise a mechanism that detects packet drop attacks staged by malicious forwarding sensor nodes.
- Perform a detailed security analysis and performance evaluation of the proposed provenance encoding scheme and packet loss detection mechanism.

Advantages of Existing System

- The fast message authentication code (MAC) schemes and Bloom filters are fixed-size data structures that efficiently represent provenance.
- Bloom filters make efficient usage of bandwidth, and they yield low error rates
- Claim for Confidentiality: - iBF is computationally infeasible to an attacker to gain data about the sensor nodes included in the provenance.
- Claim For Integrity: - An attacker, acting as single user or colluding with others in the group cannot successfully add or legitimate nodes to the data generated by the compromised/already attack happened nodes.
- An attacker or a set of cooperative attackers cannot selectively add or remove nodes from the provenance of data generated by legitimate nodes.
- A malicious aggregator cannot selectively drop a child node from the provenance.
- Claim For Freshness:- Provenance replay attacks are detected by the provenance scheme.

Disadvantages of Existing System

1. Energy wasted in en-route nodes.
2. Heavy verification burdens.
3. Gang injecting false data attack.
4. No Cooperative Authentication.

IV.PROPOSED SYSTEM

This paper proposes a novel Exact in Network Aggregation scheme for filtering for transferring multiple file. Based on the random graph characteristics of sensor node deployment and the cooperative bit-compressed authentication technique, the proposed Exact In Network Aggregation scheme can save energy by *early* detecting source and neighbouring nodes with minor extra overheads at the en-route nodes. In addition, only a very small fraction of injected false data needs to be checked by the *sink*, which thus largely reduces the burden of the *sink*. Both theoretical and simulation results are given to demonstrate the effectiveness of the proposed scheme in terms of high data

transfer probability and energy saving. To distribute the total traffic among available paths the source node performs traffic allocation based on empirical jamming statistics at individual network nodes

Advantages of Proposed System

- High filtering probability and energy saving.
- Detect injecting false data attack.
- BECAN Scheme in terms of en-routing filtering probability and false negative rate on true reports.
- Early detecting the injected false data by the en-route sensor nodes.
- Sink Verification
- Prevent/Mitigate the gang injecting false data attack from mobile compromised sensor nodes.

V.RESULTS AND DISCUSSIONS

Multi-Radio Wireless Networks

A network is assumed to consist of IEEE 802.11-based wireless links, and one control gateway. Each node is equipped with n radios, and each radio's channel and link assignments are initially made by using global channel/link assignment algorithms**.**

Link-Failure Detection/Delay Analysis

Every mesh node monitors the quality of its outgoing wireless links at every time (e.g., 10 sec) and reports the results to a gateway via a management message. Second, once it detects a link failure(s) in wireless sensor networks the failure node triggers the formation of a group among local mesh routers that use a faulty channel, and one of the group members is elected as a leader and coordinating the In network Aggregation.

Leader Node

The leader node sends a planning-request message to a gateway. If any link is failure group members send request to the particular leader after that the leader node send request to the gateway.

In Network Aggregation

The Exact In Network Aggregation scheme consists of 2 steps like multipath construction phase, Maintenance of optimal energy path to improve the energy efficiency in Sensor networks

Multipath Construction Phase

Multipath path construction phase to create a set of neighbors that is the address of all nodes that are able to transmit data from the source. In this process route request control messages are exchanged between the nodes. Each sensor node broadcasts the route request packet once and maintains its own routing table. When sensor node broadcasts a data packet to the known neighboring nodes. It doesnot maintain the whole routing information. It is necessary to store the routing information and it reduces the overhead of sensor node while it requires the proactive Protocol.

Maintenance of Optimal Energy Path

We use the concept of optimal energy path to estimate minimum energy consumption. The main aim is to maintain the data packet flow in the wireless sensor network unobstructed.

VI.CONCLUSION

This survey addressed the problem of how securely transmitting provenance for sensor networks. Based on Bloom filters this paper proposed a light-weight provenance encoding and decoding scheme. The scheme ensures confidentiality, integrity and freshness of provenance. Also this scheme extended to incorporate data-provenance joining, and to include packet sequence information that supports detection of packet loss attacks. The proposed scheme is considered as effective, light-weight and scalable. This survey plan implements a real system prototype of secure provenance scheme, and to increase the accuracy of packet loss detection, especially in the case of multiple uninterrupted malicious sensor nodes.

VII.REFERENCES

[1] I. Foster, J. Vockler, M. Wilde, and Y. Zhao, "Chimera: A Virtual Data System for Representing, Querying, and Automating Data Derivation," Proc. Conf. Scientific and Statistical Database Management, pp. 37-46, 2002.

[2] K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, "Provenance-Aware Storage systems," Proc. USENIX Ann. Technical Conf., pp. 4-4, 2006.

[3] C. Rothenberg, C.Macapuna,M.Magalhaes, F. Verdi, and A. Wiesmaier, "In-Packet Bloom Filters: Design and Networking Applications," Computer Networks, vol. 55, no. 6, pp. 1364-1378, 2011.

[4] R. 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.

[5] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure Data Aggregation in Wireless Sensor Networks," IEEE Trans. Information Forensics and Security, vol. 7, no. 3, pp. 1040-1052, June 2012.

[6] Y. Simmhan, B. Plale, and D. Gannon, "A Survey of Data Provenance in E-Science," ACMSIGMODRecord, vol. 34, pp. 31-36, 2005.

[7] A. Ramachandran, K. Bhandankar, M. Tariq, and N. Feamster, "Packets with Provenance," Technical Report GT-CS-08-02, Georgia Tech, 2008.

[8] W. Zhou, M. Sherr, T. Tao, X. Li, B. Loo, and Y. Mao, "Efficient Querying and Maintenance of Network Provenance at Internet- Scale," Proc. ACM SIGMOD Int'l Conf. Management of Data, pp. 615-626, 2010.

[9] W. Zhou, Q. Fei, A. Narayan, A. Haeberlen, B. Loo, and M. Sherr, "Secure Network Provenance," Proc. ACMSOSP, pp. 295-310, 2011.

[10] A. Syalim, T. Nishide, and K. Sakurai, "Preserving Integrity and Confidentiality of a Directed Acyclic Graph

Model of Provenance," Proc. Working Conf. Data and Applications Security and Privacy, pp. 311-318, 2010.

[11] 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.

[12] S. Chong, C. Skalka, and J.A. Vaughan, "Self-Identifying Sensor Data," Proc. Ninth ACM/IEEE Int'l Conf. Information Processing in Sensor Networks (IPSN), pp. 82-93, 2010.

[13] T. Wolf, "Data Path Credentials for High-Performance Capabilities- Based Networks," Proc. ACM/IEEE Symp. Architectures for Networking and Comm. Systems, pp. 129-130, 2008.

[14] R. Laufer, P. Velloso, D. Cunha, I. Moraes, M. Bicudo, M. Moreira, and O.Duarte, "Towards Stateless Single-Packet IP Traceback," Proc. 32nd IEEE Conf. LocalComputer Networks (LCN), pp. 548-555, 2007.

[15] P. Jokela, A. Zahemszky, C. Esteve, S. Arianfar, and P. Nikander, "LIPSIN: Line Speed Publish/Subscribe Inter-Networking," Proc. ACM SIGCOMM Conf. Data Comm., pp. 195-206, 2009.

[16] A. Ghani and P. Nikander, "Secure In-Packet Bloom Filter Forwarding on the Netfpga," Proc. European NetFPGA Developers Workshop, 2010.