SAJET

South Asian Journal of Engineering and Technology Vol.2, No.15 (2016) 102–110

ISSN No: 2454-9614

Constructing Log file to Avoid Packet Drop Attacks in WSNs

B. Poovizhi[a], J. Jeyaram[a*]

[a)] *Department of Computer Science and Engineering, Vivekanandha Institute of Engineering and Technology for Women, Tiruchengode , Tamilnadu, India.*
[b)] *Department of Computer Science and Engineering, Vivekanandha Institute of Engineering and Technology for Women, Tiruchengode , Tamilnadu, India.*

*Corresponding Author: B.Poovizhi

E-mail: poovizhispersonal @gmail.com,
Received: 17/11/2015, Revised: 20/12/2015 and Accepted: 05/03/2016

Abstract

Large-scale sensor networks are deployed in numerous application domains, and the data they collect are used in decision-making for critical infrastructures. Data are streamed from multiple sources through intermediate processing nodes that aggregate information. A malicious adversary may introduce additional nodes in the network or compromise existing ones. Therefore, assuring high data trustworthiness is crucial for correct decision-making. Data provenance represents a key factor in evaluating the trustworthiness of sensor data. Provenance management for sensor networks introduces several challenging requirements, such as low energy and bandwidth consumption, efficient storage and secure transmission. A novel lightweight scheme to securely transmit provenance for sensor data. The proposed technique relies on in-packet Bloom filters to encode provenance. The efficient mechanisms for provenance verification and reconstruction at the base station. The secure provenance scheme with functionality to detect packet drop attacks staged by malicious data forwarding nodes. The proposed technique was evaluated both analytically and empirically, and the results prove the effectiveness and efficiency of the lightweight secure provenance scheme in detecting packet forgery and loss attacks.

Keywords: Provenance, security, sensor networks.
Reviewed by* **ICETSET'16 *organizing committee*

1. Introduction

Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. The architecture of the internet, when modified can reduce the possible attacks that can be sent across the network. Knowing the attack methods, allows for the appropriate security to emerge. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms. The businesses create an

"intranet" to remain connected to the internet but secured from possible threats.

Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet. There are currently two fundamentally different networks, data networks and synchronous network comprised of switches.

The internet is considered a data network. Since the current data network consists of computer- based routers, information can be obtained by special programs, such as "Trojan horses," planted in the routers. The synchronous network that consists of switches does not buffer data and therefore are not threatened by attackers. That is why security is emphasized in data networks, such as the internet, and other networks that link to the internet. When developing a secure network, the following need to be considered:

1. Access – authorized users are provided the means to communicate to and from a particular network
2. Confidentiality – Information in the network remains private
3. Authentication – Ensure the users of the network are who they say they are
4. Integrity – Ensure the message has not been modified in transit
5. Non-repudiation – Ensure the user does not refuse that he used the network

1.1. Wireless Sensor Networks

A Wireless Sensor Network is a self-configuring network of small sensor nodes communicating among themselves using radio signals, and deployed in quantity to sense, monitor and understand the physical world. Wireless Sensor nodes are called motes. WSN provide a bridge between the real physical and virtual worlds. Allow the ability to observe the previously unobservable at a fine resolution over large spatiotemporal scales. Have a wide range of potential applications to industry, science, transportation, civil infrastructure, and security.

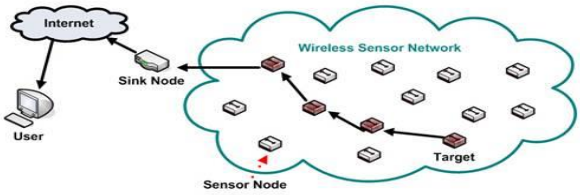

Fig.1 Wireless sensor network

The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network.

1.2 Applications

- Habitat and Ecosystem Monitoring
- Seismic Monitoring

• Civil Structural Health Monitoring
• Monitoring Groundwater Contamination
• Rapid Emergency Response
• Industrial Process Monitoring
• Perimeter Security and Surveillance
• Automated Building Climate Control

1.3 Characteristics

The main characteristics of a WSN include:

- Power consumption constraints for nodes using batteries or energy harvesting
- Ability to cope with node failures (resilience)
- Mobility of nodes
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to with stand harsh environmental conditions
- Ease of use
- Performance can be measured
- Reliability

1.4. Security in Sensor Networks

Wireless sensor networks (WSN) are generally set up for gathering records from insecure environment. Nearly all security protocols for WSN believe that the opponent can achieve entirely control over a sensor node by way of direct physical access. Security goals in sensor networks depend on the need to know what we are going to protect. We determine four security goals in sensor networks which are Confidentiality, Integrity, Authentication and Availability (CIAA).

- Confidentiality is the ability to conceal message from a passive attacker, where the message communicated on sensor networks remain confidential.
- Integrity refers to the ability to confirm the message has not been tampered, altered or changed while it was on the network.
- Authentication Need to know if the messages are from the node it claims to be from, determining the reliability of message's origin.
- Availability is to determine if a node has the ability to use the resources and the network is available for the messages to move on.

1.5 Attacks in Wireless Sensor Networks

- Node Capture Attack

- Denial Of Services (Dos)
- Software Attacks
- Routing Attacks
- Traffic Analysis Attacks
- Sybil Attacks
- Attacks On In-Network Processing
- Attacks On Time Synchronization Protocols
- Replication Attacks

2. Data Provenance in Sensor Networks

Sensor networks are used in application domains, examples are cyber physical infrastructure, environmental monitoring, whether monitoring power grids, etc. The data that should be large sensor node sources and processed in-network with their way to a Base Station (BS) that performs which decision should be taking. Information is considered in the decision process or making.

Data provenance is an effective method to assess data trustworthiness, and the actions performed on the data. We investigate the problem of secure and efficient provenance transmission and handling for sensor networks, and we use provenance to detect packet loss attacks staged by malicious sensor nodes. In a multi-hop sensor network the data provenance is to allow the Base Station to trace the source and forwarding path of a specific data packet the provenance must be record for each an every packet, but important challenges arise due to some reason the first is tight storage, energy and bandwidth constraints of sensor nodes. Therefore it is necessary devise a light-weight provenance solution with low overhead. Sensors should operate in un-trusted environment, where they may be happens subject to attacks. That's why it is necessary to address security requirements such as privacy, reliability and cleanness of provenance. Our project goal is to design a provenance encoding and decoding tool that would be satisfies such safety and presentation needs.

We Design propose a provenance encoding strategy where each node on the track of a data packet securely embeds provenance information within a Bloom filter that is conveyed along with the data. Receiving the packet the Base Station should be extracts and verifies the provenance information. The provenance encoding system that allows the Base Station to detect if a packet drop attack was staged by a malicious node. We use fast Message Authentication Code and Bloom filters (BF), which are stable size data structures that efficiently represent provenance wireless networks of sensor devices Sensor networks of the future are intended to consist of hundreds of cheap nodes that can be readily deployed in physical situations to collect useful information.

Our motivation on the subsection of distributed networking applications created on packet header-size Bloom filters to share some state between network nodes. The specific state carried in the Bloom filter differs from application to application, ranging from secure credentials to IP prefixes and link identifiers with the shared

requirement of a fixed-size packet header data structure to well verify set memberships. Bloom filters make effective usage of bandwidth, and they yield low error rates in practice. Our specific contributions are:-
We formulate the problem of secure provenance transmission in sensor networks.

- The implementation of an in-packet Bloom filter provenance encoding Scheme.
- To design efficient techniques for provenance decoding and verification at the base station.

2.1 Packet Drop Attacks

The Simplicity in Wireless Sensor Network with resource constrained nodes makes them extremely vulnerable to variety of attacks. In a Wireless sensor networks sensor nodes monitor the environment, detect events of interest, produce data and collaborate in forwarding the data towards to a sink, which could be a gateway, base station or storage node. Securing the Wireless Sensor Networks need to make the network support all security properties: confidentiality, integrity, authenticity and availability.

A sensor network is often deployed in an unattended and hostile environment to perform the monitoring and data collection tasks. When it is deployed in such an environment, it lacks physical protection and is subject to node compromise. After compromising one or multiple sensor nodes, an adversary may launch various attacks to disrupt the in-network communication. Among these attacks, two common ones are dropping packets and modifying packets, i.e., compromised nodes drop or modify the packets that they are supposed to forward.

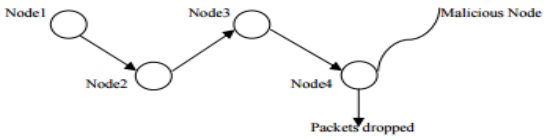

Fig.2 Packet drop attack

Packet dropping is nothing but a bad node drops all or some of the packets that are supposed to be forwarded. It may also drop the data generated by itself for some malicious purpose such as blaming innocent nodes. This paper proposes a scheme to catch both packet droppers and modifiers. At first routing tree is established using DAG. Data is transmitted along the tree structure toward the sink. A packet sender or forwarder adds a small number of extra bits, which is called packet marks, is designed such that the sink can obtain the dropping ratio associated with every sensor node. Node categorization algorithm to identify nodes that are droppers / modifiers for sure or are suspicious droppers/ modifiers. The packet dropping attack can be classified into several categories in terms of the strategy adopted by the malicious node to launch the attack.

- The malicious node can intentionally drop all the forwarded packets going through it (black hole).
- It can selectively drop the packets originated from or destined to certain nodes that it dislikes.
- A special case of black hole attack dubbed gray whole attack is introduced.
- In this attack, the malicious node retains a portion of packets (one packet out of N received packets or one packet in a certain time window), while the rest is normally relayed.

3. Secure Transmission Process

A novel lightweight scheme to securely transmit provenance for sensor data. Furthermore, as an enhancement the secure provenance scheme with functionality to detect packet drop attacks staged by malicious data forwarding nodes. The ip address of the node to which the data packet is transmitted is used as the secret key. This technique relies on in-packet Bloom filters to encode provenance.

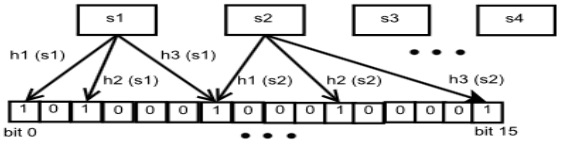

Fig.3 Bloom Filter

The BF is a space-efficient data structure for probabilistic representation of a set of items. Some applications that use Bloom filters need to communicate these filters across the network. In this case, besides the three performance metrics we have seen so far : (1) The computational overhead to lookup a value (related to the number of hash functions used), (2) The size of the filter in memory, and (3) The error rate, a fourth metric can be used: the size of the filter transmitted across the network. The bloom filter uses the IP address as a key and encodes the data packet for transmission. Hence the attacker cannot decrypt the data without knowing the key value. The proposed technique was evaluated both analytically and empirically, and the results prove the effectiveness and efficiency of the light weight secure provenance scheme in detecting packet forgery and loss attacks.

3.1 System architecture

The data packet is transmitted from the sender to the receiver. The node has encrypted with the key. At receiving site the file has asked for the key to decrypt the packet. If the packet receives at the correct site with the key value, the content displayed. Otherwise an encrypted format is displayed. And a packet drop attack acknowledgement is send to the sender.

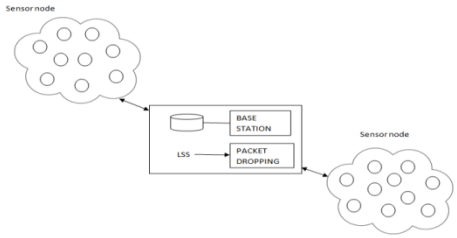

Fig.4 System Architechture

3.2 Network Model

Consider a multihop wireless sensor network, consisting of a number of sensor nodes and a base station that collects data from the network. Sensor nodes are stationary after deployment, but routing paths may change over

time, e.g., due to node failure. Each node reports its neighboring (i.e., one hop) node information to the BS after deployment. Assume a multiple-round process of data collection .Each sensor generates data periodically, and individual values are aggregated towards the BS using any existing hierarchical (i.e., tree-based) dissemination scheme Sensor nodes are stationary after deployment, but routing paths may change over time, e.g., due to node failure.

3.3. Provenance Encoding

For a data packet, provenance encoding refers to generating the vertices in the provenance graph and inserting them into the iBF. Each vertex originates at a node in the data path and represents the provenance record of the host node. A vertex is uniquely identified by the vertex ID. The VID is generated per-packet based on the packet sequence number (seq) and the secret key Ki of the host node. A block cipher function is used to produce this VID in a secure manner.

3.4. Provenance Forgery and Packet Drop Attacks

The secure provenance encoding scheme is extended to detect packet drop attacks and to identify malicious node (s). Assume the links on the path exhibit natural packet loss and several adversarial nodes may exist on the path. For simplicity, consider only linear data flow paths. Also, the issue of recovery is not addressed once a malicious node is detected. Existing techniques that are orthogonal to our detection scheme can be used, which initiate multipath routing for may build a dissemination tree around the compromised nodes. A provenance encoding is augmented to use a packet acknowledgement that requires the sensors to transmit more meta-data.

For a 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 there is an intermediate packet drop, some nodes on the path do not receive the packet. Hence, during the next round of packet transmission, there will be a mismatch between the acknowledgements generated from different nodes on the path. This fact is used to detect the packet drop attack and to localize the malicious node. Consider a data flow path P where nl is the only data source. The link between nodes ni and nðiþ1Þ are denoted as li. Provenance encoding and decoding for detecting packet loss are described in next module.

3.5. Provenance Decoding

Not only the intermediate nodes, but also the BS stores and updates the latest packet sequence number for each data flow. Upon receiving a packet, the BS retrieves the preceding packet sequence transmitted by the source node from the packet header, fetches the last packet sequence for the flow from its local storage and utilizes these two sequences in the process of provenance verification and collection. Provenance BS first executes the provenance verification process upon receiving a packet. The BS knows the current data path for the packet (decoded from the provenance of the previous packet in the flow), and the preceding packet sequence number forwarded by each node in the path. In this context, the BS assumes that each node in the path saw and forwarded the same packet in the last round, and that this packet's sequence number is the same one as recorded at the BS.

Thus the verification is bound to fail when pSeq and pSeqb do not match, which also indicates a possible packet loss and suffices to execute provenance collection process directly skipping the verification. Verification failure here indicates either a change in the data flow path, a packet drop attack or a BF modification attack, and triggers the provenance collection process. Collection attempts to retrieve the nodes from the encoded provenance, confirm a packet loss and identify the malicious node that dropped the packet. It also distinguishes between the packet drop attack and other attacks that might have altered the iBF. The step by step of the overall process is represented in this figure

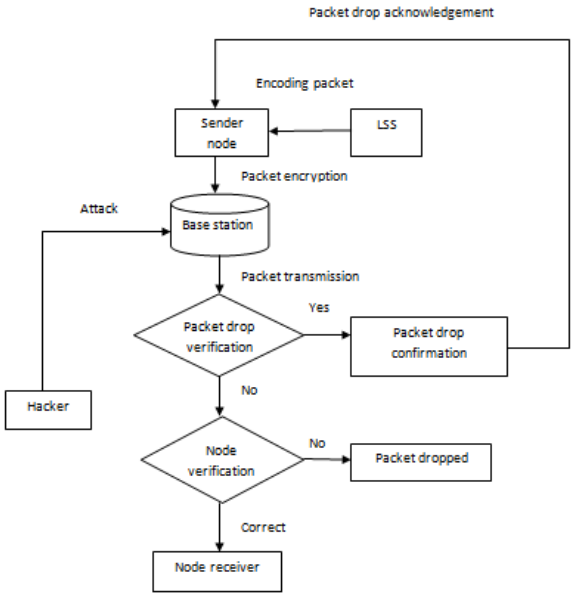

Fig.5 Data flow diagram

4. Conclusion

The problem of securely transmitting provenance for sensor networks, and proposed a light-weight provenance encoding and decoding scheme based on Bloom filters. The scheme ensures confidentiality, integrity and freshness of provenance. We extended the scheme to incorporate data-provenance binding, and to include packet sequence information that supports detection of packet loss attacks. Experimental and analytical evaluation results show that the proposed scheme is effective, light-weight and scalable.

In future proposed system, a log key of this secure provenance scheme to be used to improve the accuracy of packet loss detection, especially in the case of multiple consecutive malicious sensor nodes.

ACKNOWLEDGMENT

This research was supported by my Head of the Department, Prof.T.R.Srinivasan. We thank Mr.Chandra Mohan for assistance with a technique, and Mr.Sathish for comments that greatly improved the manuscript. We thank famous persons Dr.Karunanithi and Dr.K.C.K.Vijayakumar, for sharing their pearls of wisdom with us during the course of this research, and we thank Mr.J.Jeyaram and Mr.R.Rajagopal reviewers for their so-called insights. We also immensely grateful to family for their comments and support, although any errors are our own and should not tarnish the reputations of these esteemed persons.

References

[1] H. Lim, Y. Moon, and E. Bertino, "Provenance-Based Trustworthiness Assessment in Sensor Networks, "Proc. Seventh Int'l Workshop Data Management for Sensor Networks, pp. 2-7, 2010.

[2] 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.

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

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

[5]] 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.

[6] S. Madden, J. Franklin, J. Hellerstein, and W. Hong, "TAG: A Tiny Aggregation Service for Ad-Hoc Sensor Networks," ACM SIGOPS Operating Systems Rev., vol. 36, no. SI, pp. 131-146, Dec. 2002.

[7] K. Dasgupta, K. Kalpakis, and P. Namjoshi, "An Efficient Clustering Based Heuristic for Data Gathering and Aggregation in Sensor Networks,"Proc. Wireless Comm. and Networking Conf., pp. 1948-1953, 2003.

[8]] S. Sultana, E. Bertino, and M. Shehab, "A Provenance Based Mechanism to Identify Malicious Packet Dropping Adversaries in Sensor Networks," Proc. Int'l Conf. Distributed Computing Systems (ICDCS) Workshops , pp. 332-338, 2011.

[9] L. Fan, P. Cao, J. Almeida, and A.Z. Broder, "Summary Cache: A Scalable Wide-Area Web Cache Sharing Protocol," IEEE/ACM Trans. Networking, vol. 8, no. 3, pp. 281-293, June 2000.

[10] A. Kirsch and M. Mitzenmacher, "Distance-Sensitive Bloom Filters,"Proc. Workshop Algorithm Eng. and Experiments, pp. 41-50, 2006.

[11] 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.

[12] M. Garofalakis, J. Hellerstein, and P. Maniatis, "Proof Sketches: Verifiable In-Netwok Aggregation, "Proc. IEEE 23rd Int'l Conf.Data Eng. (ICDE), pp. 84-89, 2007.