Volume 6, Issue 3, March 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Provenance Forgery attack, Packet Drop and Detection methods in Wireless Sensor Network– A Case Study

D. Sowmyadevi*
Dept. of Computer Science
Sri Ramakrishna College of Arts and Science for Women, Coimbatore,
Tamilnadu, India

Dr. K. Karthikeyan
Dept. of Computer Science
Government Arts and Science College
Karambakudi, Pudukkottai Dt.
Tamilnadu, India

Abstract: ***Wireless Sensor Network is broadly used in many application domains. These nodes collect data from many sensor nodes. There are many promising attacks like provenance forgery, Packet drop attack, DDos attack, Jamming attack etc. are found in the WSN while transmitting the data. 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 keeps log information of data about who accessed this data, who modified this data, the path from the data is traversed etc. Data provenance has important role in the evaluation of trustworthiness of data therefore, it is important to secure data provenance. The packet drop attack can be frequently deployed to attack wireless sensor network. The malicious router can also accomplish this attack selectively. The several challenging requirements for provenance management and packet drop attacks in sensor networks are low energy and low bandwidth consumption, competent storage and secure transmission. In this paper focus on Provenance Forgery attack, Packet Loss and Detection methods in Wireless Sensor Network.***

Keywords: Wireless sensor network, Provenance forgery attack, Packet Drop attack, Bloom Filter, Data Provenance.

I. INTRODUCTION

In a wireless sensor network, data are produced at a large number of sensor node sources and processed in network at intermediate hops network on their way to a Base Station that performs decision-making. The diversity of data sources create the need to assure the trustworthiness of data such as only trustworthy information is considered in the decision process. Sensor nodes monitor the environment, detect events of interest, produce data and collaborate in forwarding the data towards a sink, which could be a gateway, base station, storage node, or querying user. 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 [11] to disrupt the in-network communication. In a multi-hops sensor network and data provenance allows the BS to trace the source and forwarding path of an individual data packet. Provenance must be recorded for each packet, but important challenges arise due to the tight storage, energy and bandwidth constraint of sensor nodes. Therefore, it is necessary to devise a light-weight provenance solution with low overhead. Hence it's necessary to address security requirements like confidentiality, integrity and freshness of provenance. Our important goal is to design a provenance encoding and decoding method that satisfies security and performance need. To deal with packet droppers, a broadly adopted countermeasure is multi-path forwarding in which each packet is forwarded along multiple redundant paths and hence packet dropping in some but not all of these paths can be tolerated. This scheme introduces high extra communication overhead.

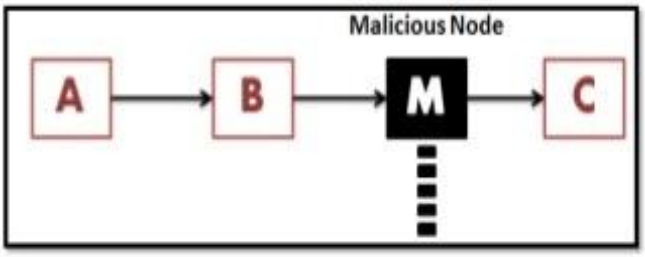

Fig1: Packet Drop Attack

Wireless sensor network has several limitations each node has limited battery, limited bandwidth to communicate, limited processing power and limited memory. Existing system to detect the provenance forgery attack considered such limitations of the WSN therefore it is efficient system for this task. Several WSN routing protocols are simple and are vulnerable to attacks from those works on routing in ad hoc networks. Most threats against WSNs fall into one of the following groups:

(i) Spoofed, altered, or replayed routing information
(ii) Selective forwarding
(iii) Sinkhole attacks
(iv) Sybil attacks
(v) Wormholes
(vi) HELLO flood attacks
(vii) Acknowledgment spoofing

II. LITERATURE SURVEY

In packet Bloom filters encode scheme is used for data provenance. 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. Introduce efficient mechanisms for provenance verification and reconstruction at the base station. In addition, extended the secure provenance scheme with functionality to detect packet drop attacks staged by malicious data forwarding node [1] and evaluated the proposed technique 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.

Data provenance is enhanced in sensor network using in packet bloom filter. The scheme ensures confidentiality, integrity and freshness of provenance. Initially performs provenance at the base station then perform reconstruction of the data at the base station [2]. The provenance scheme functionality used to detect packet drop attacks organized by malicious data forwarding nodes by extending to incorporate data-provenance joining, and to include packet sequence information that supports detection of packet loss attacks.

Provenance encoding strategy is used to preserve integrity and confidentiality of provenance database, whereby each node on the path of a data packet securely embeds provenance information within a Bloom filter that is transmitted along with the data. The Base station extracts and verifies the provenance information [3]. Also devise an extension of the provenance encoding scheme that allows the Base station to detect if a packet drop attack was staged by a malicious node.

Efficient tools used for provenance verification method and reconstruction method at the base station with the functionality to detect [4] packet drop attacks or by malicious data forwarding nodes. Propose a novel lightweight scheme to securely transmit provenance for sensor data and suggest 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.

Data are produced at a large number of sensor node sources and processed in-network at intermediate hops on their way to a base station that performs decision-making. The diversity of data sources creates the need to assure the trustworthiness of data. Data provenance is an effective method to assess data trustworthiness. [5] focused on the problem of secure provenance transmission in sensor networks, and identify the challenges specific to this context by implementing Message Authentication Code (MAC) schemes and Bloom filters and perform a detailed security analysis and performance evaluation of the proposed provenance encoding scheme and packet loss detection mechanism by representing unique sequence number per packet and provenance encoding and decoding at the base station.

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. To identify the Packet Droppers and Packet Modifiers [6] ranking algorithms and packet marks were used. The Performance is represented using detection rate and false positive probability. The Proposed scheme provides an effective mechanism for catching compromised node.

Packet dropping and modification are common attacks that can be launched by an adversary to disrupt communication in wireless multi-hop sensor networks. A simple yet effective scheme is used which can identify misbehaving forwarders that drop or modify packets. According to the scheme, a dynamic routing tree rooted at the sink is first established. When sensor data is transmitted along the tree structure towards the sink, each packet sender or forwarder adds a small number of extra bits, which is called packet marks [7], to the packet. Based on the packet marks, the sink can figure out the dropping rate associated with every sensor node. Node Categorization Algorithm used to identify nodes that are droppers/modifiers for sure or are suspicious droppers/modifiers.

MANETs have become a commonly used network for various applications. But this advantage suffers with serious security concerns, mainly a wireless transmission medium perspective where such networks may be subject to packet dropping. Mobility and portable nature of Mobile Ad hoc Network may also lead to link failure. During packet forward, valuable packets may be dropped by malicious nodes present in the network. Link error and malicious packet dropping are the two sources for packet losses in MANET. [8] Introduces a new protocol named secured Ad hoc on demand distance vector (SAODV), which can truthfully detect packet dropping attack in MANET. SAODV can detect malicious nodes by identifying dropping of routing and data packet. Packet dropping due to both link error and presence of malicious nodes can detect by SAODV. It also provides importance to preserve privacy of data.

Provenance handling of continuous data needs to cover various issues, admitting the storage efficiency, processing throughput, bandwidth conception and secure transmission. These challenges are handled by providing secure and

efficient transmission of provenance along with sensor data by embedding it over the inter packet delays (IPDs). The embedding of provenance within a host medium makes this technique reminiscent of watermarking. Spread-spectrum [9] based watermarking technique is proposed, that avoids data degradation due to traditional watermarking. Provenance is extracted effectively based on an optimal threshold mechanism that minimizes the probability of provenance decoding error.

In a multi-hop sensor network, data provenance allows the base station to trace the source and forwarding path of an individual data packet since its generation. Provenance must be recorded for each data packet, but important challenges arise due to the tight storage, energy and bandwidth constraints of the sensor nodes. Therefore, it is necessary to devise a light-weight provenance solution which does not introduce significant overhead. A novel light-weight scheme to securely transmit provenance for sensor data assuring high data trustworthiness in such a context is crucial for correct decision-making. A provenance encoding strategy [10] whereby each node on the path of a data packet securely embeds provenance information within a Bloom filter, which is transmitted along with the data, the base station extracts and verifies the provenance.

III. METHODOLOGY

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. The problem of secure provenance transmission in sensor networks proposes an in-packet Bloom filter provenance encoding scheme. Each sensor node generates data periodically, and individual values are routed and aggregated towards the BS using any existing hierarchical dissemination scheme. Each data packet contains a unique packet sequence number, a data value and provenance. The sequence number is attached to the packet by the data source, and all nodes use the same sequence number. The sequence number integrity is ensured through message authentication codes (MAC). To satisfy security and performance, provenance encoding and decoding mechanism were designed. In provenance encoding strategy each node on the path of a data packet securely embeds provenance information within a Bloom filter that is transmitted along with the data. Upon receiving the data, the base station (BS) extracts and verifies the provenance and proposed efficient mechanisms for provenance verification and reconstruction also at the base station.

In Provenance Verification mechanism, the BS conducts the verification process not only to verify its knowledge of provenance but also to check the integrity of the transmitted provenance. The Provenance Collection mechanism verifies the data to ensure its origin, and rejects the data if the verification fails at the base station. This encoding scheme allows the BS to detect packet drop attack organized by a malicious node by binding provenance data with each packet by using Provenance Collection algorithm.

IV. RESULT

To solve the problem of securely transmitting provenance for sensor networks, proposed a light-weight provenance encoding and decoding scheme based on Bloom filters. The security features of the scheme include confidentiality, integrity and freshness and performed a detailed security analysis and performance evaluation of the proposed provenance encoding scheme, packet loss detection mechanism and malicious node Identification. Bloom filters make efficient usage of bandwidth, and they yield low error rates and represent provenance. The results prove the effectiveness and efficiency of the lightweight secure provenance scheme in detecting packet forgery and loss attacks.

V. CONCLUSION

This paper describes the need of provenance data for data transmitted in network and the need of securing this provenance data, extended the scheme to incorporate data-provenance binding and to include packet sequence information that supports detection of packet loss attacks in WSNs. It also shows the various methods to save more energy and bandwidth. This paper goal is to improve the mechanism of provenance in wireless sensor networks by delivering the efficient transmission of secure provenance data along the transmitting medium, free from external threats.

REFERENCES

[1] Sultana. S, Ghinita. G, Bertino. E and Shehab. M, "A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks," IEEE Transactions On Dependable And Secure Computing, Vol. 12(3):256-269, May/June 2015.

[2] Tharani. M, Sivachandran. K and Saranya. S.N, "An Efficient Detection of Forgery And Packet Drop Attacks In Wireless Sensor Networks," International Journal of Advanced Information and Communication Technology (IJAICT), Vol. 2(7): 1055-1058, November 2015.

[3] Adhau. R, Ambekar. A, Drakshe. A and Thorave. R, "Detecting Attacks in Wireless Sensor Network through Bloom Filtering," International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 6(5): 4397-4399, 2015.

[4] Kadam. M, Dakhore. S, Chavan. K and Bandgar. A, "A Secure Model For Detecting Origin Forgery And Packet Drop Attacks In WSN," Multidisciplinary Journal of Research in Engineering and Technology, Vol. 2(4): 823-828, 2015.

[5] Dinde. R, Jain. A, Thorkar. S, Patil. A "Provenance Forgery and Packet Drop Attacks Detection in Wireless Networks," International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), Vol. 4(2): 2560-2565, February 2016.

[6] Kumar. K.B and NarasimhaReddy. V, "Identification of Packet Dropping and Modification in Wireless Sensor Networks," International Journal of Computational Engineering Research, Vol. 03(7):1-6, 2013.

[7] Wang. C, Feng. T, Kim. J, Wang. G and Zhang. W, "Catching Packet Droppers and Modifiers in Wireless Sensor Networks," IEEE Computer Society, Vol. 23(5): 835-843, April 2012.

[8] George. N and Sujitha. M, "Truthful Detection of Packet Dropping Attack in MANET," International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4(7):317-320, July 2015.

[9] Ramya. K P, Revathi. M.K and Devi. C.R, "PINCODE: Protection in Provenance Conduction Over Data Stream for Sensor Data," International Journal of Research in Engineering & Advanced Technology (IJREAT), Vol. 1(5): 1-7, Oct-Nov 2013.

[10] Sultana. S, Ghinita. G, Bertino. E, Shehab. M, "A Lightweight Secure Provenance Scheme for Wireless Sensor Networks," IEEE Computer Society-International Conference on Parallel and Distributed System, pp.101-108, 2012.

[11] Vanitha. N and Jenifa. G, "Detection of Packet Droppers in Wireless Sensor Networks Using Node Categorization Algorithm," International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3(3):69-74, March 2013.

