EXPLORATIONS ON ENGINEERING LETTERS (EEL)
VOLUME 1, ISSUE 1 (2016):PP.79-84
SANA ACADEMIC PRESS

Detecting Provenance Forgery and Packet DropAttacks in Wireless Sensor Network

D.Thalapathi[1], P.Chidambaranathan[2], R.Latha[3]
[1]Research Scholar, St.Peter'sUniversity, Chennai.
[2]Asst.Prof.&Head., Dept. of Computer Applications, St.Peter's University, Chennai
[3]Prof.&Head., Dept. of Computer Science & Applications, St.Peter's University, Chennai
d.thalapathi@gmail.com

Abstract*-For numerous applications large-scale sensor networksare deployed. The data collected in these applications are used for critical infrastructures in decision making. Streamed data from multiple sources through intermediate nodes are obtained as aggregate information. Malicious adversary is introduced as additional nodes in the network. Data provenance allows the base station to trace the source and to forward the 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 constraints of sensor nodes. Furthermore, sensors often operate in an entrusted environment, where they may be subject to attacks. Hence, it is necessary to address security requirements such as confidentiality, integrity and freshness of provenance. The goal is to design a provenance encoding and decoding mechanism that satisfies such security and performance needs. This research propose a provenance encoding strategy 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. Upon receiving the packet, the base station extracts and verifies the provenance information. It also devise an extension of the provenance encoding scheme that allows the BS to detect if a packet drop attack was staged by a malicious data forwarding nodes. For more security linear congruential generator is to be implemented:*
*An LCG is essentially a formula of the following form:number = (a * number + c) mod m*

Keywords: *Provenance, Bloom Filter, Base Station, Malicious Node.*

I. INTRODUCTION

Wireless Sensor Networks have great potential for numerous applications such as military target tracking and surveillance, natural disaster relief, health monitoring and hazardous environment exploration and seismic sensing. Wireless sensor network stream both continuous and discrete data or monitor events. In a network, a node can create data, process the data such as fusion, pass the data along.A wireless sensor network is a collection of self-organized sensor nodes. Provenance this method embedded the provenance information within a bloom filter that is transmitted along the data. On obtaining the packet the base station will check the information and it also check the packet drop attack. Data provenance gives a detailed record of the derivation of a piece of data. The trust of data depends on the trust of the node that creates the data and the trust of the nodes the data has visited. Two example wireless sensor network applications are a battlefield monitoring system and a

supervisory control data acquisition system. A battlefield system gathers target locations from multiple sources such as cameras, satellite images, vehicles, proximity sensors. Critical decisions are taken based on the data hence trustworthiness is a concern and can be assessed by using provenance. The efficient mechanism of provenance in WSNs as provenance represents a key factor in evaluating the trustworthiness of sensor data. Data provenance plays an important role for assuring data trustworthiness. Provenance helps gather, share and store the information which may lead to privacy and security concern in wireless sensor network. Security is one of the main characteristic of wireless sensor network affected with any attacks. Provenance, a mechanism of trust and reputation evaluation is an indispensable component to enhance the security of the entire network. Since provenance records the history of data acquisition and transmission, it is considered as an effective mechanism to evaluate the trustworthiness and security of the data. It also provides the information about the operations performed on data. Provenance function is also deals with the detecting malicious node in network and to detect the packet drop in network. Provenance of sensor data is critical in many applications as it: plays a key role in assessing and ensuring data trustworthiness, aids in preventing data losses, ensures the repeatability of scientific experiments and processes; and helps in preventing and investigating scientific frauds.

Compression provenance scheme is vital in wireless sensor network to control the bandwidth and energy consumption. Arithmetic coding (Syed Rafiul Hussain,2014) for secure data provenance compression is a good method. Arithmetic coding is a lossless data compression technique that assigns short code words to more probable data symbols and longer code word to less probable ones. Arithmetic coding scheme uses floating point number to support a limited numbers of bits to represent the digit after its decimal point. Trust is the challenging area in wireless sensor network as it is used in military operation. Distributed intelligence works faster in network, which uses centralized approach and it is self adjusting information network, dataflow produce more accurate. Distributed system which evaluates the trust in the network that is more flexible and more responsive, which enhance the network trust in network. As trust is monitored and network is continuously restructured, our network remains trustworthy for a longer time. In a dictionary based provenance scheme, each sensor node in the network stores a packet path dictionary. Which contain database of the provenance information as path indexes instead of the path itself in the provenance.This index is stored in a dictionary. With the support of this dictionary, a fixed size path index can be used to represent a path of arbitrary length. This technique gives secure provenance compression for wireless sensor network. ERUPT method aim is to reduce the energy consumption and to develop the trustworthy provenance in WSN. This method determine a routing tree rooted at the base station with reduced number of active sensing nodes and select energy efficient paths while ensuring that the selected paths contain trustworthy nodes and exhibit low correlation among them.

II. SYSTEM DESCRIPTION

The system securely transmit provenance for sensor data and the technique relies on in-packet Bloom Filters to encode provenance. An efficient mechanism for provenance verification and reconstruction at the base station is introduced. In addition, the secure provenance scheme with functionality to detect packet drop attacks staged by malicious data forwarding nodes is extended. It proposes an in-packet Bloom Filter provenance encoding scheme. The problem of secure provenance transmission in sensor networks, and identifies the challenges specific to this context, the secure provenance encoding scheme and devise a mechanism that detects packet drop attacks staged by

malicious forwarding sensor nodes. The design efficient techniques for provenance decoding and verification at the base station.The detailed security analysis and performance evaluation of the proposed provenance encoding scheme and packet loss detection mechanism. A multihop wireless sensor network, consisting of a number of sensor nodes and a base station that collects data from the network. 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 for a given round. The sequence number integrity is ensured through message authentication code. The various modules in the proposed system is given below.

Client and Server Configuration – In this module wireless sensor network using network sensors that can transmit data to server via gate way. Gateway is intermediate server in between wireless sensor network and main server. Sensors send packet when detect abnormal condition, server take action based on that values.

Packet Encryption – Spliting large data into small packets, each packet contain sensor province, sensor value, sensor id. Bloom filter data structure for effectively data transmission between the source and destination, and also each packet contains unique identification number. That number must be encrypted before start transaction. For encryption this research uses linear congruential generator. A linear congruential generator is essentially a formula of the following form:
number = (a * number + c) mod m
In other words, begin with some start or "seed" number which ideally is "genuinely unpredictable", and which in practice is "unpredictable enough". For example, the number of milliseconds - or even nanoseconds - since the computer was switched ON is available on most systems. Then, each time need a random number, and multiply the current seed by some fixed number, a, add another fixed number, c, then take the result modulo another fixed number, m. The number a is generally large.

Packet Split using Bloom Filter – Bloom Filters, which are fixed-size data structures that compactly represent provenance. Bloom Filters make efficient usage of bandwidthand they yield low error rates in practice. The packets are split by using Bloom Filter before sending to the Gateway.

Packet Drop Detection – The packet drops are identified easily in the Main Server. When the hacker alters the packet data in the Gateway.The value of the packets will be altered. Once the data is transmitted to the Main Server from the Gateway, the transmitted packets are decrypted. During the decryption of the packets if there is any alteration in the packet in the Gateway there will be the Packet Drop.

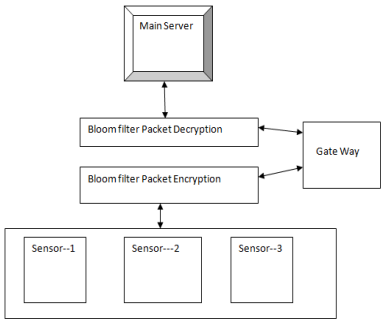

Figure 1 Block Diagram of the System

III. SYSTEM IMPLEMENTATION AND RESULTS

Implementations are made using J2EE.The following four characteristics must follow to be an Object Oriented language.

• **Inheritance –** It is the process of creating the new classes and using the behavior of the existing classes by extending them just to reuse the existing code and adding addition a features as needed.

•**Encapsulation –** It is the mechanism of combining the information and providing the abstraction.

• **Polymorphism –** As the name suggest one name multiple form, Polymorphism is the way of providing the different functionality by the functions having the same name based on the signatures of the methods.

• **Dynamic binding –**It is the way of providing the maximum functionality to a program about the specific type at runtime.

Java platform have graciously designed two ways of creating threads. One by implementing an interface and other by extending a class.Extending a class is the way Java inherits methods and variables from a parent class. In this case, one can only extend or inherit from a single parent class. This limitation within Java can be overcome by implementing interfaces, which is the most common way to create threads.

Interfaces provide a way for programmers to lay the groundwork of a class. They are used to design the requirements for a set of classes to implement. The interface sets everything up, and the class or classes that implement the interface do all the work. The different sets of classes that implement the interface have to follow the same rules.

For simulation a WSN module is created. The network scenario contains provenance, sensor number, and sensor value. Initially a key is requested via main server through gateway node for encryption. Gateway node is an intermediate server in between wireless sensor network and main server. Split the larger data into smaller packets, each packet contain sensor province, sensor value, and sensor id. Bloom filter is used that is present in the wireless sensor network for encryption which effectively transmits data between the source and destination. Also each packet contains unique identification number. The encrypted value is sent to the main server. For encryption/decryption linear congruential generator is used. The linear congruential server is present in the main server. Bloom filters, which are fixed-size data structures that compactly represent provenance. The packets are merged by using Bloom filter before sending to the Gateway node. The packet drops are identified easily in the main server. When the hacker alters the packets data in the Gateway node, the value of the packets will be altered. Once the data is transmitted to the main server from the Gateway node the encrypted packets are decrypted using Bloom filter that is present in the main server. Then the transmitted packets are decrypted. During the decryption of the packets if there are any alteration in the packet in the Gateway it can be easily identify that the packets are modified by the hacker.

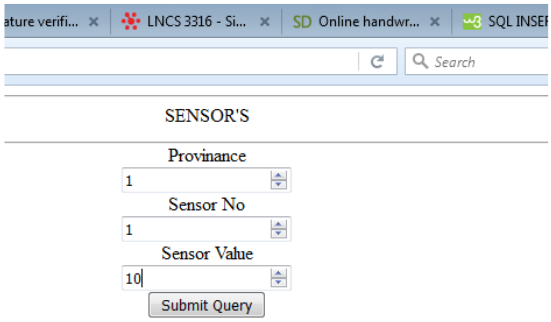

Figure 2 Sensor Page

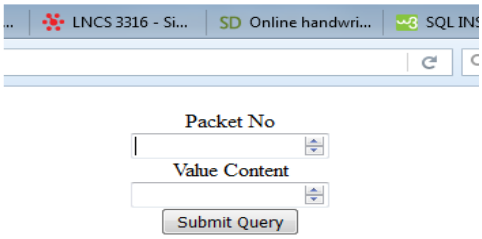

Figure 3 Gateway Page

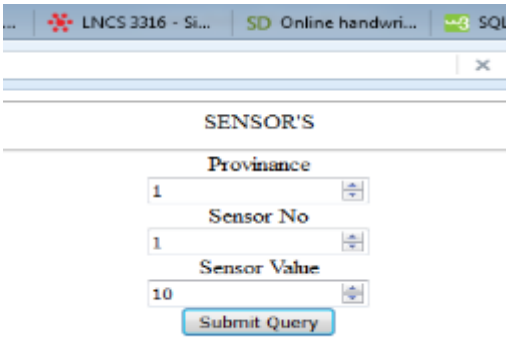

Figure 4 Sensor Sending Data through Gateway

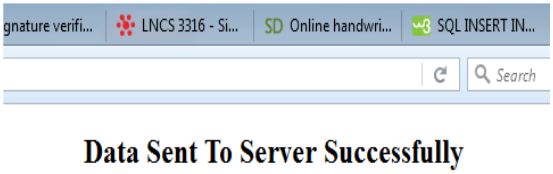

Figure 5 Gateway Sending Data to Main Server

IV.CONCLUSION

The problem of securely transmitting provenance for sensor networks, and proposed a provenance encoding and decoding scheme based on Bloom Filters is addressed. The scheme ensures confidentiality, integrity and freshness of provenance. The scheme to incorporate data-provenance binding and to include packet sequence information that supports detection of packet loss attacks is extended. Experimental and analytical evaluation results show that the proposed scheme is effective, light-weight and scalable. As future work, implement a real system prototype of our secure provenance scheme, and to improve the accuracy of packet loss detection, especially in the case of multiple consecutive malicious sensor nodes.

REFERENCES

1. AlamS. I. and Fahmy.S, ―A Practical Approach for Provenance Transmission in Wireless Sensor Networks, Ad hoc Networks, Vol. 16, No. 0, pp. 28-45, 2014.

2. Devika.Mand Priyanka, ―A Survey of Provenance Management in Wireless Sensor Network, International Journal of Engineering Research and Applications, Vol. 6, No. 1, Part – 5, pp. 91-93, January 2016.

3. Changda Wang, Elisa Bertino,Syed RafiulHussain, Salmin Sultana, and, ―Secure Data Provenance Compression Using Arithmetic Coding in Wireless Sensor Networks, 2014.

4. Gulustan Dogan,Jin-Hee Cho, Kannan Govindan, Mohammad MaifiHasan Khan, PrasantMohapatra, Theodore Brown, TarekAbdelzaher, ―Evaluation of Network Trust Using Provenance Based on Distributed Local Intelligence in 2011 military communication conference track 4-middleware services and application.

5. David YauK. Y,Iftekharul AlamS. M, and Sonia Fahmy, ―ERUPT: Energy-efficient trustworthy Provenance Trees for Wireless Sensor Networks, IEEE, 2014.

6. Kannan Govindan and PrasantMohapatra, Xinlei Wang, ―Provenance-based Information Trustworthiness Evaluation in Multi-hop Networks, IEEE globecom-2010.

7. Bertino.E,Ghinita.G, and Sultana.Shehab S.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. 99, 2014.