International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: http://dx.doi.org/10.7324/IJERAT.3163

E-ISSN : 2454-6135

Vol.3 (12) Dec -2017

A Secure Scheme for Detecting Provenance Forgery and Masquerade Attack in Wireless Sensor Networks

A. Priyadharshini [1] and A. Sekar [2]

[12]Assistant Professor

[1] Department of Information Science and Engineering

CMR Institute of Technology

Bangalore, Karnataka

[2] Department of Computer Science and Engineering

Knowledge Institute of Technology

Salem, Tamil Nadu

India

ABSTRACT

The sensor networks are popularly increasing and it used as a effective way in decision making infrastructures such as Data Acquisition systems, Supervisory Control industrial monitoring, battlefield monitoring systems. It is difficult for the process to maintain the trustworthiness of the data. To address this problem, we propose a systematic technique for evaluating the trustworthiness of data. This approach uses the data provenance and it provides quantitative measures for trustworthiness. The encoded method is used in the provenance approach as sensor data travels through intermediate sensor nodes. Then it is decoded and verified at the base station. The is also able to protect from The harm from malicious attacks such as packet dropping is also be protected by the provenance technique and the responsible node for packet drops is also detected. As such it makes possible to modify the route to avoid nodes that could be compromised or malfunctioning. Another major issue is a Masquerade attack. The masquerade attack, where an attacker takes on the identity of a confirming the user to maliciously utilize that user's privileges, obtain a serious threat to the security of information systems. Therefore a large number of attempts has been made at detecting these attacks; yet achieving high levels of accuracy remains an open challenge. In this work, Data Driven Semi-Global Alignment (DDSGA) approach is used to detect the masquerade attack.

Keywords: *Masquerade Attacks, Data provenance, Data driven semi global alignment.*

1. INTRODUCTION

Wireless Sensor Network (WSN) provides a wide range of applications in areas such as environment monitoring, medical care, in hospitable terrain, traffic monitoring, robotic exploration, and agriculture surveillance, and security systems. The wireless Sensor network is the collection of sensor nodes that send the data to the base station. Sensor nodes sense the information based on the phenomena such as temperature, pressure, humidity, etc. Sensor nodes are defined as motes. It has been in variety of applications from volcano detection, surveillance, environmental monitoring etc. The key challenges in sensor networks are storage, energy efficiency, privacy and security.

Among these challenges, the security creates the lots of problems in wireless sensor networks. In order to transfer information between the points radio waves are used in most of the wireless communication technology which are known as nodes. One application domain of wireless communication is wireless sensor networks. WSN is a distributed system, containing resource or constrained nodes that work in an ad hoc manner using multi- hope communication. WSNs and Internet are integrated as a new emerging area called Internet of Things (IoT), which resolves all the issues in the day to day life. IoT encourages several novel and existing applications such as public safety, medical and health care, home and office security, transportation, environment monitoring, infrastructure management and military applications.

As sensor network information could also be altered by mistreatment compromising nodes therefore integrity controls should make sure that information received has not been altered till it reaches its original destination. Individual will modify the data through malicious node and alter the packet data before its destination and will send false information to the receiver. Wireless sensor networks provide one of the most important functions is data gathering. The sensor readings are collected from the sensor nodes to the sink.

The key contribution of provenance in systems has been highlighted in the recent research work, where the use of untrustworthy data may lead to catastrophic failures in sensor networks. Data provenance is the newest term used in sensor network. Provenance refers to the origin or the source of the data. Provenance in sensor network is not properly addressed. Data provenance is also used to detect packet loss. Data provenance allows the Base station to trace the source and forwarding path of an individual data packet in wireless sensor network. Provenance must be recorded for each packet. Data provenance is a effective tool to calculate data trustworthiness because it summarizes the history and the actions performed on the data. But it is one of the important challenges arise due to the energy and bandwidth constraints and tight storage of sensor nodes. Therefore it is essential for lightweight provenance.

Among the networking attacks masquerade attack causes the vulnerable to the network. The masquerade attack is kind of attack, where the attacker act like the legitimate person/ authorized person and access the resource with full privilege. Masquerading attack can cause serious damage to the computational framework and computer systems. A masquerade attack that can be the most serious form of computer abuse. Masquerade detection used to builds a profile for each user by gathering information the user behaviour of sensor network. Gather information such as location, session duration, CPU time, login time, commands issued, user ID and user IP address. While the success of this approach has been limited, most of the reports do not make clear the origins of errors made by the detection mechanisms. The following method is used to detect the packet loss, secure data provenance and it is prevent from masquerade attacks.

The remaining section of this paper is formalized as follows. Related work is discussed in Section 2. Then our proposed mechanism is proposed in Section 3. The paper is concluded in Section 4. Finally, the paper describes the future enhancement in Section 5.

2. LITERATURE REVIEW

Hyo-Sang Lim,Yang-Sae Moon and Elisa Bertino[4] proposes the approach that uses the data provenance as well as their values in generating trust scores, that is, quantitative measures of trustworthiness. It obtain the trust scores, it proposes a cyclic framework which well reflects the inter-dependency property. The trust score of the network nodes is affected by that created and updated node, and vice-versa. The trust scores of data items are generated from their value similarity and provenance similarity. The value similarity is given by the principle that “the uttermost homogeneous values, the higher the trust scores, for the same event”. The provenance similarity is defined on the principle that “the higher the trust scores, the most different data provenances with similar values”. The main flaw is that this strategy and multi-attributes in-network operations and is multiple dependent attributes are not dealt and other probability distributions instead of normal distributions are not considered [4].

The design and implementation of ExSPAN [10], that efficient network provenance is achieved by a generic framework in a distributed environment. To “explain” the existence of any network state it utilizes the database notion of data provenance, such that an adaptable operation is provided by a network provenance. That flexibility can be accomplished at Internet, ExSPAN uses the declarative networking in continuous queries over distributed streams are modeled and will be done and declared concisely in a declarative query language. The provenance to enable distribution at Internet has been developed in database that has extended existing data models, numerous optimization techniques are explored to query distributed network provenance and manage and efficiently. The ExSPAN prototype is developed using Rapid Net, is used in networking platform based on the emerging ns-3 toolkit. The main drawback is does not provide confidentiality and authenticity of provenance information [10].

The major security threat to the data traffic is malicious packet [1] dropping attack in the sensor network, since it may obstruct the legal propagation of sensitive data and decreases network throughput. Dealing with this attack is challenging since the unreliable wireless communication.

Distinct features and resource constraints of the sensor network may mislead to some erroneous resolution and cause communication disaster about the presence of such attack. This method uses a mechanism based on data provenance to identify the attack; the source of the attack is identified in addition to that, i.e. the malicious node. For this purpose, the characteristics of the watermarking based provenance have been utilized after the provenance embedding and also depend on the inter-packet timing characteristics. The scheme consists of three phases

(i) Detection of Packet Loss
(ii) Identification of Attack Presence
(iii) Localization the Malicious Node/Link.

Based on the distribution of the inter-packet detain the closing of packet will be found.

By comparing the empirical average packet loss rate with the natural packet loss rate of the data flow path the presence of the attack is determined. The more provenance information is transmitted along with the sensor data to isolate the malicious link.

If the observed behaviour, reportedly of a specific user, and the learnt pattern of this user's past data does not match then Masquerade attack [1] will be reported. The major limitation in this process is that the user may legitimately deviate temporarily from the past behaviour. If the eccentricity is big and near-permanent, then it is desirable that such deviations are captured in a detection mechanism. This aspect of user behaviour while detecting masquerade attacks is also taken into consideration in this method.

The proposed scheme is based on the premise that the commands that have been used by a legitimate user or an attacker and the trained signature may differ. But the deviation of an attacker persists longer whereas that of the deviation of the legitimate user is momentary.

The existing system doesn't properly address the provenance in sensor networks. Provenance must be recorded for each packet, due to the bandwidth constraints, energy and tight storage, and of sensor nodes important challenges may arise. For each user masquerade detection builds a profile by gathering information such as location, login time, session duration, CPU time, commands issued, user ID and user IP address. Then, these profiles against logs and signals are compared as an attack any behaviour that does not match the profile.

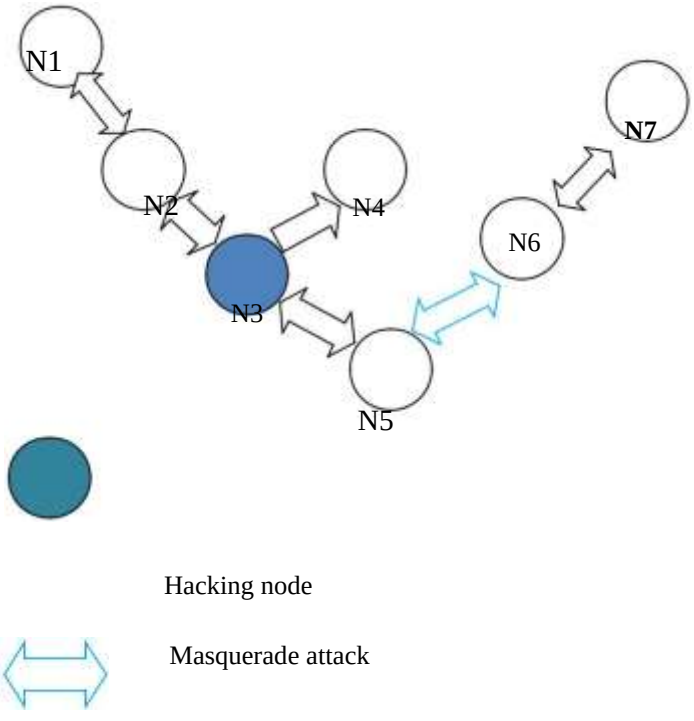

Fig 1: Masquerade attack scenario

2.1 **Problem in existing system**

The level of accuracy and performance have not been achieved by the current detection approaches for practical implementation regardless of the huge amount of information they used to build a profile such as mouse movements, opened files names, command line commands, system calls**,** opened windows title, and network actions. Disadvantage of the existing system is (i) A malicious adversary may introduce additional nodes in the network (ii) Semi Global alignment in masquerade detection has not reached the accuracy and performance of large scale systems.

3. IMPLEMENTATION AND ITS METHODOLOGY

In proposed system using key exchanging, cryptography, and signature technique are used in secure scheme for detecting provenance forgery and DDSGA detecting masquerade attack in wireless sensor networks. So easily identify the suspicious data for sensor network. In verify module identify the suspicious data and provenance data. Acquiring packet data malicious data means placed in suspicious box in sensor network. Suppose data will be provenance data means placed in provenance box for sensor network. In addition to this work, Data Driven Semi-Global Alignment (DDSGA) approach, this improves both the computational performance and detection accuracy of the Enhanced-SGA and of HSGAA to detect the Masquerade attacks. Major advantage for the proposed system are (i) It controls the malicious attack done by the masquerade attacks (ii) It improves the accuracy of packet loss detection, exclusively in the case of multiple consecutive malicious sensor nodes in sensor network(iii)It securely transmits the provenance for sensor data The modules of this approach are given below.

3.1 Encryption

In data provenance approach light-weight in-packet Bloom filters are used and are put into code as sensor data navigate through midway sensor nodes, and are decrypted or decoded and verified at the base station. In this first module it encodes or encrypts the provenance in a distributed aspect within the data packet, and decrypts it at the base station. Each data packet consists of its own data, a sequence number, and an in-Bloom filter (iBF) field containing the provenance in the sensor network.

The following encryption and decryption mechanism uses the RSA Algorithm. Consider Alice and Bob as a source node and data node.

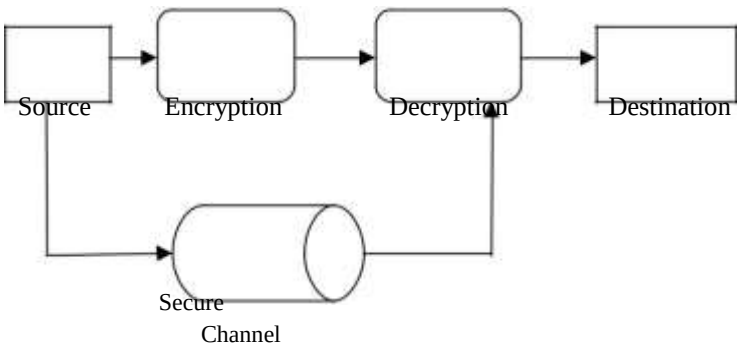

Fig 2: Encryption Method

Alice transmits her public key (n, e) to Bob and hold back the exclusive key secret. Bob is then in a need to send message M to Alice. M is first turned into an integer m, such that $0 \leq m < n$ by applying padding scheme which is a reversible protocol. Cipher text c corresponding to m is then computed

$$c = m^e \pmod{n} \qquad \text{----------} \qquad (1)$$

This can be done quickly using the method of exponentiation by squaring. Bob then impart c to Alice. The relatively nine values of m could yield a cipher text c equal to m, but in practice this is very unlikely to occur.

3.2 SIGNATURE PROCESS

The data producer sets up its signing key k and data consumer the verification key k0 in a utmost secure mode will be fixed that forbid malware from accessing the secret keys in the system for verified the signature using algorithm is DSS (Digital signature scheme). The data producer signs its data D with a secret key k, and outputs D along with its proof sig. Key k0 is used by the data consumer to verify the signature sig of received data D such that the origin is ensured and the data is rejected if the verification fails.

3.3 DECRYPTION

In the receiver side they receive the encoding data and it performs decryption operation based on the following methods.

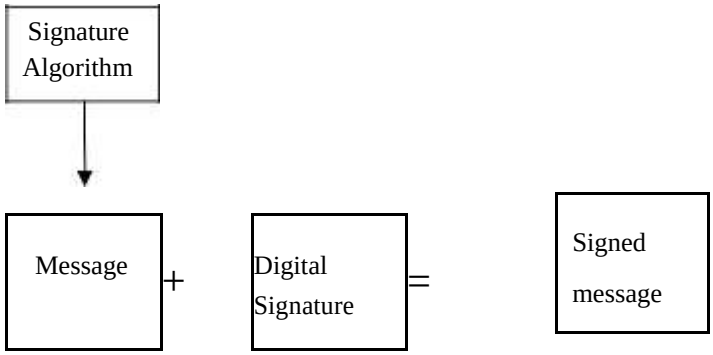

Fig 3: Authentication Checking

m is recovered from c by using Alice's private key exponent d via computing

$$m = c^d \pmod{n} \tag{2}$$

Given$m$, she can recover the original message M by reversing the padding scheme.

3.4 PROVENANCE COLLECTION

When the base station receives a data packet it checks for all possible safe paths from the source node of this packet in data provenance. These paths have been previously saved by the base station in sensor network. In the propose system the receiver module obtain a packet data suspicious means place in suspicious box suppose data correct data means placed in province box.

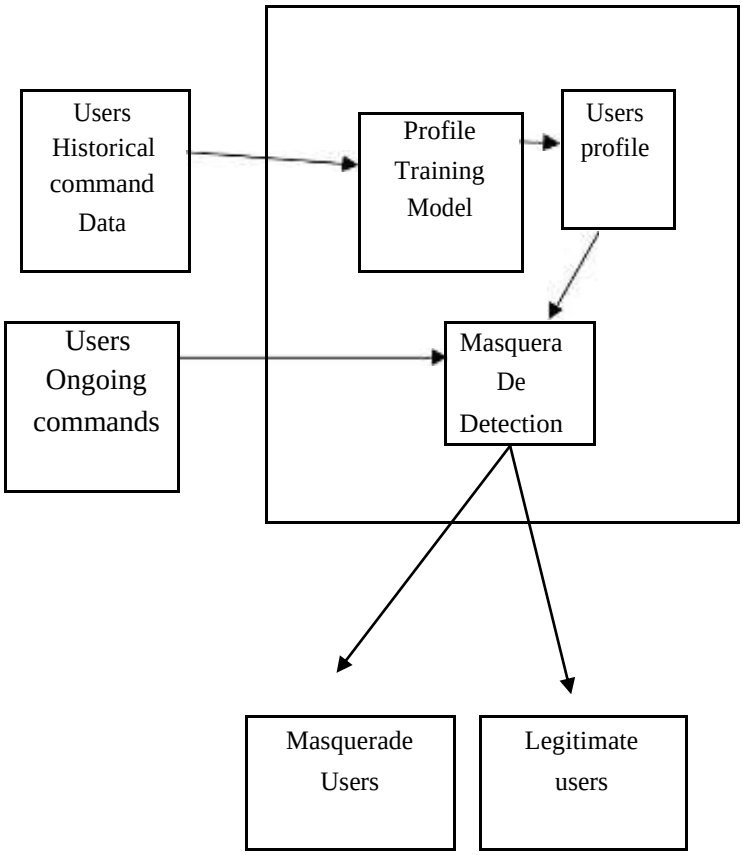

Fig 4: Masquerade attack detection

3.5 Masquerade Attack Detection

DDSGA is a masquerade detection approach based upon Enhanced-SGA (Semi Global Alignment) approach. It aligns the user active session sequence to the previous ones of the same user and it labels the misalignment areas as anomalous in sensor network. A masquerade attack is signalled if the percentage of anomalous areas is bigger than a dynamic, user dependent edge for detection in wireless sensor network. In tiny alterations in the user sequences with slight changes can be tolerated in the low level representation of user commands and it is disintegrated into a configuration phase, a detection phase and an update on the DDSGA approach. The configuration phase, computes, for every user, the alignment specification to be used by both the detection and update phases. In DSS algorithm the detection phase arranges the user ongoing session to the signature sequence. The computational performance and accuracy of this phase is enhanced by two ways former is the Top-Matching Based Overlapping (TMBO) and the latter is parallelized approach. In the update phase, DDSGA prolong both user lexicon lists with the new patterns and the user signatures and to reconfigure the system parameters in the Enhanced-SGA. In this module node can be protected from the masquerade attack. Another, these methods detect the packet dropping in the sensor networks.

3.6 Detecting Packet Drop

The nodes that are droppers /modifiers in sensor nodes are found and categorized by the sink for detecting packet drop in sensor network using the secure scheme. The behaviour of nodes such as user login time, commands issued, location, session duration, CPU time and with the information accumulated in sink user ID and user IP address are traced in variety of scenarios, it classifies the nodes as droppers /modifiers for sure or suspicious droppers /modifiers in sensor network.

3.7 Malicious Node Identification

Malicious behaviour of the node is broadcasted throughout the network. Then data to the malicious node are not forwarded by any node in the network. A sensor node will not allow the data from a malicious node. The malicious nodes can be easily revealed by nearby nodes. The malicious node has been detected in a trusted manner.

4. CONCLUSION

This work enhances the light weight scheme that transmits the provenance for sensor data securely. The proposed approach utilizes the encryption and decryption method in order to encode the provenance that simplify the verification of provenance and is reconstructed at the base station. Furthermore, with the functionality of packet dropping attacks this work extends the secure provenance scheme. Another method it uses the Data-Driven Semi-Global Alignment (DDSGA) approach that improves the detection precision and the computational efficiency of the Enhanced-SGA and of HSGAA. Considering the alignment of the active session sequence to the recorded sequences of the same user is the core idea of DDSGA. Label the areas as abnormal and several anomalous areas are a strong indicator of a masquerade attack after discovering the misalignment areas. DDSGA improves the efficiency in security by using not only lexical matching such as longest common substring, searches string matching but also using the small mutations in the sequences with trivial changes in the low-level representation of the user commands. This method also identifies the packet loss and data is also encrypted using the digital signatures.

5. FUTURE ENHANCEMENTS

For future work, we plan to apply our approach to detect masquerade attacks in cloud environment by improving our CIDS framework. As a first step, we have developed a new data set, CIDD that includes distinct audit data from physical network environment and distinct host operating systems. This in turn will provision an evaluation of DDSGA that can use different kinds of audit sequences.

REFERENCES

[1] A. S. Sodiya, O. Folorunso, S. A. Onashoga, and P. O. Ogundeyi, “An improved semi-global alignment algorithm for masquerade detection,” Int. J. Netw. Security, vo1. 12, no. 3, pp. 211–220, May 2011.

[2] Hisham A. Kholidy, Fabrizio Baiardi, and Salim Hariri, Member, IEEE Computer Society “DDSGA: A Data-Driven Semi-Global Alignment Approach for Detecting Masquerade Attacks “IEEE Transactions on Dependable and Secure Computing, Vol. 12, no. 2, March/April 2015.

[3] Hisham A. Kholidy and Fabrizio Baiardi, “CIDS: A framework for intrusion detection in cloud systems,” in Proc. 9th Int. Conf. Inf. Technol.: New Generations, Las Vegas, Nevada, USA, Apr. 2012, pp. 16–18.

[4] 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.

[5] Salmin Sultana, Gabriel GhinitaElisa Bertino, Fellow, IEEE , and Mohamed Shehab, “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, no. 3, may/june 2015

[6] Subrat Kumar Dash, K. S. Reddy, and K. A. Pujari, “Adaptive Naive Bayes method for masquerade detection”, Security Commun. Netw., vol. 4, no. 4, pp. 410–417, 2011.

[7] S. E. Coulla and B. K. Szymanski, “Sequence alignment for masquerade detection,” J. Comput. Statist. Data Anal., vol. 52, no. 8, pp. 4116–4131, Apr. 2008.

[8] 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.

[9] 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.

[10] 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.