ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 7, July 2016

Lightweight Scheme for Detection and Identification for Provenance Forgery Attack in WSN

Ashutosh Bajpei, Prof.Geetika Narang

***Abstr*act - Many application domains use Wireless Sensor Network. Data collected from many sensor nodes which is passed through the intermediate node and aggregated at single node and collected data is used for decision making. The most important part in the WSN transmission is the security and integrity and confidentiality of the transmitted data. There are many possible attack found in the WSN while transmitting the data like provenance forgery, Packet drop attack, DDos attack, Jamming attack and many others. Data provenance keeps log information of data that accessed this data, who modified this data, path from which data is traversed etc. Data provenance takes important role in the evaluation of trustworthiness of data. Our work is focused on forgery attacks on provenance data. Existing system able to detect the forgery attack using bloom-filter data structure and also can detect packet drop attack. Existing system cannot identify the provenance forgery attacker. Our work proposed novel scheme which detects the provenance forgery attack and also identifies the attacker.**

Keywords **- Wireless sensor network, provenance forgery, forgery attacker**.

I. Introduction

Data is generated or sensed at the sensors in wireless sensor network. Generated data at sensors send to base station for decision making. For example huge server house installed with temperature sensor and cooling infrastructure. Sensors sense the temperature and send it to the base-station, on the basis of received data base-station controls cooling infrastructure. As the whole system depends on the received data, communication between sensor and base station must be secure. In WSN, network is ad hoc type made up of all active sensors in the network. When data needs to send from one sensor to base station, if sensor is not in the range of base station then data is passes through other sensors in the network. As there is no direct communication between sensor and base station, data transfer depends on the in between sensors reduces the trust on the received data at the base station. Data provenance keeps records of history of ownership of data. At base station data provenance[1] is used to check the trustworthiness of received data

Due to importance of provenance data to evaluate the trustworthiness it is suffered from forgery attack[3]. Using provenance data it is important to detect the provenance forgery before evaluating trustworthiness of data. Wireless sensor network has several disadvantages 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[5] therefore it is efficient system for this task. Limitation of existing system is that it can-not identify the attacker who did the provenance forgery. To overcome this limitation of the existing system, we proposed system which is extension of existing system which has ability to identify the attacker and inherits lightweight nature from existing system.

II. Literature Survey

Ramachandran [1] proposed Pedigree provenance scheme in which each packet is tagged with provenance data. With provenance data tagger is deployed at each host which tags each packet. Paper [1] used provenance data for traffic classification, Arbiter is deployed at each host which decides what to do with received packets with specific tags Packet classification before Pedegree is mainly dependent on the IP addresses and port numbers but after pedigree it used tag information on the tags for packet classification. Pedigree scheme does not consider adversary network case and hence cannot deal with forgery attacks in the WSN.

Paper [2] discussed that network accountability, failure analysis is important for network management and need of network provenance. In distributed environment Paper [2] proposed ExSPAN provenance system. ExSPAN used data provenance to prove the state of the network. ExSPAN was developed using rapidnet which is based on ns3 toolkit Experimental results shows that system is generic and extensible. Same as Pedegree [1] this scheme also did not consider security of the provenance data.

Wenchao Zhou [3] et.al observed the need of securing the provenance and proposed scheme Secure Network provenance which gives proof for the state of the provenance data. Network operator can detect faulty

nodes and also can assess the damage to network from such faulty nodes. Snoopy named SNP is proposed in paper and experimental results shows that Snoopy can prove state of provenance data in malicious WSN model SNP scheme did not considered the disadvantages of WSN i.e. limited bandwidth , low battery and low memory.

Paper [4] discussed the need to find source of the data which is sent over the internet and proposed a scheme which provides strong integrity and confidentiality of provenance data. Proposed scheme is designed in such way that it can be deployed at application layer Experiments shows that it can providing integrity and confidentiality to provenance data results into overload with range 1% to 13%.Proposed system gives control over the visibility of provenance data and assures no one can modify the provenance data without detection. Through encryption and incremental chained signature mechanism integrity and confidentiality is achieved.

Paper [5] proposes method to secure directed acyclic graph of the provenance data. Proposed method used digital signature in which provenance owner and processors tags or signs nodes. And by checking the signatures relationship between provenance data graph and integrity is validated. Both paper [4] and [5] are generic solutions which can be apply any network and they are not designed with consideration of nature of WSN

Paper [6] proposed a mechanism in which sensor data is tagged with its provenance data automatically and provenance data can be recover from this tagged data. Experiments with different scenarios proved robustness of this scheme. Special feature of this scheme is provenance data is embedded into actual sensor data. Proposed system does not provide any way to provide security to provenance data.

Paper [7] focuses on provenance management and proposed novel secure provenance transmission scheme in which provenance is embedded into inter packet timing domain and also considers disadvantages, requirements of WSN. Proposed scheme is different from traditional watermarking schemes scheme embeds provenance data into in inter-packet delays and not in actual sensor data. As provenance data is not directly embedded into actual data, data quality degradation problem is solved. Provenance information is recovered using optimal threshold bases mechanism to reduce the provenance recovery errors. Proposed scheme is based on the spread spectrum watermarking technique Proposed scheme is efficient against various sensor network or flow watermarking attacks. Proposed scheme assume that provenance data remains same for flow of the packets.

Paper [8] discussed the design of the bloom filter data structure and its efficiency. Bloom filter is vector of n bits. When data is encoded into bloom filter set of hash functions is used. Data to be encoded is hashed using hash function. Output of the hash function will be integer values. Initially bit vector contains all bit value equal to 0 Bit at output integer index is set to 1. To check the membership of element is the main purpose of bloom filter is i.e. once element is encoded; membership of the data can be checked. Papers [8] describe the potential network applications of bloom filter data structure and describe suitability of the bloom filter for network applications.

Paper [9] focuses on security of the provenance data specific to wireless sensor network Paper proposed scheme to detect forgery against on provenance data, detection of packer drop attack and can also identify the attacker of packer drop attack. For encoding provenance data proposed scheme uses in packet bloom filter data structure. To encode the provenance data to in packet bloom filter 3 hash functions are used. Use of bloom filter data structure results into lightweight scheme and which is suitable to wireless sensor network. Each packer consists of sequence id of the packet, actual sensor data and n-bit bloom filter vector. ID of the each node in path is encoded into bloom filter vector to detect the forgery attack. It is assumed that base station knows the path of the received packet. When packet is reached at the base station in the WSN, fresh bloom filter is taken and encoded with all nodes in the path. If generated bloom filter and bloom filter extracted from received packet are same then there is no forgery attack else there is forgery attack. Actual sensor data is also secured along with provenance data with proposed scheme in this paper. The effectiveness and its lightweight nature of the scheme proved by experimental results

III. Proposed System

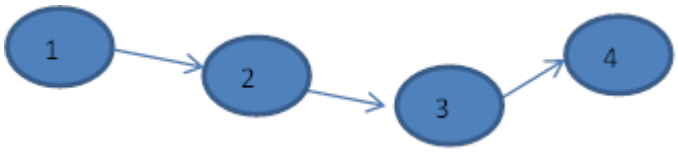


Fig. 1 Simple path in network

Existing system detects provenance forgery attack but cannot identify the attacker. Proposed system identifies the provenance forgery attacker. System uses following methodology.

System has two phases one is encoding, another is detection phase which detects the attack and also identifies attacker.

3.1 Encoding phase:

1) When data is sent from source to destination, bloom filter vector is generated for each node in the path.

2) Provenance data i.e. Vid of the node is encoded on the next node in the network.

Below figure shows simple path in the network in which Node 1 is sender and BS is destination. For each node in the path separate bloom filter is generated. Each packet consists of sequence number of packet which is generated by source of packet, data in the packet and set of bloom filter vectors. Each bloom filter is encoded with Vid; Vid is generated using Node id of previous node and private key of current node by applying AES algorithm on it.

For example if node 1 is source and BS is destination. Sequence number, data and black bloom filter is sent to node 2 by node 1. When packet comes at node 2 then Vid is generated using Node id 1 and private key pk2 of node 2.

Vid1 = generateVID1 (1, Sequence ID) (1)

Generated Vid is encoded in to the blank bloom filter bf1, with this Vid three distinct hash functions are used for encoding. Encoding of Vid to the bloom filter is same as existing system.

Now packet contains sequence id, data and one bloom filter bf1 in the bloom filter vector. Updated packet is send to next node in the network i.e. node 3. When packet is received at node 3 then fresh bloom filter is generated and encoded with Vid which is generated using Node id 2 and private key pk3 of node 3.

Vid is encoded in bloom filter. To support our attacker identifier technique, in bloom filter, along with encoding Vid, we have added one more field called as encrypted encoding E. E is sum of indexes where 1 is marked in bloom filter of previous node in encrypted form.

3.2 Steps in Generating E are as follows:

Initially at first node bloom filter is empty. Then at second node Vid is encoded as described above. But before marking the index of encoded Vid, we generate the E. Here E1 will be 0 as initially bloom filter is blank. So at second node E1 is 0. Then at third node we will have two bloom filters of its previous nodes. Now we calculate sum of indexes of 1's in all previous node's bloom filters. Now E2 has some value in it. Ei goes incrementing with the number of nodes. At Base station Ek will have sum of 1's indexes of all bloom filters of the nodes in path this procedure will continue till packet reaches to the base station BS. When packet reaches to the Base station it contains sequence id, data and vector of n bloom filters where n is number of nodes in the path.

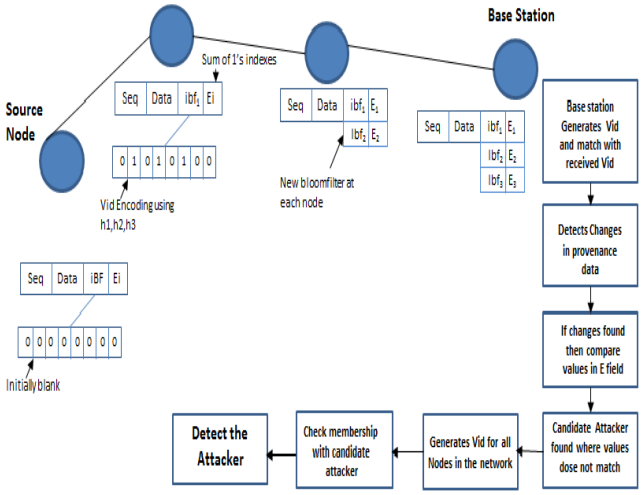


Fig. 2 Architecture of Proposed System

3.3 Detection and identification phase:

It is assumed that BS knows the path from which packet is traversed.

At base station first step is to generate vector of encoded bloom filters. For each node separate bloom filter is encoded and stored in the vector.

In second phase each bloom filter in the received bloom filters vector is checked in reverse order with respective generated bloom filter in previous step. If any of the bloom filters does not match then provenance forgery is detected and if all bloom filters are matched with received bloom filters then there is no forgery attack.

Then values in field E is matched with respective value of E of each received bloom filters. If value is not matched in any bloom filter, then that node is considered as candidate attacker.

Vid is generated for all nodes in the network considering the case if the attacker is not in the path. Then we check all nodes membership with candidate attacker. Matched node identified as an attacker as it has its address encoded with candidate attacker.

IV Mathematical Model

Input Set {I1, I2, I3, I4}

I1: Packet data

I2: Blank bloom filter and empty E field, Node id of previous node and private key of current node.

I3: Received VBfr and Base Station generated Vbf

I4: Vid of all m nodes in the network and candidate attacker.

Process Set {P1, P2, P3, P4, P5, P6, P7, P8, P9, P10}

P1: Packet reach to first node; Bloom filter is created at each node, blank at first node

P2: To support attacker detection technique, Field E is attached to each bloom filter consist of sum of indexes marked as 1 of all previous bloom filters

P3: Generates Vid for each node using node id of previous node and private key of the current node.

Vid = generateVid (Node ID of i-1, Private Key of ith node)

P4: This Vid is encoded in bloom filter using h1, h2, h3 three hash functions and E is updated accordingly.

P5: Generate Vector of bloom filter with values E for all nodes at base station

P6: Compare received vector of bloom filter with this Vector of bloom filter.

P7: Match values in E if any changes is detected.

P8: Consider node as a candidate attacker where values in E are not matched.

P9: Generate Vid for all nodes in the network.

Vid = generateVid (NodeID of (i-1) th node, Private Key of ith Node)

P10: Check membership of each candidate attacker with each Vid to find the attacker.

Output Set {O1, O2, O3, O4, O5}

O1: Blank bloom filter with empty E field is created.

O2: Generation of vector of Bloom filter Bf containing generated Vid and encoding of bloom filter using three hash functions and sum of E fields.

O3: Candidate attacker

O4: Set of vector of bloom filter containing Vid for m nodes.

O5: Attacker Detection from m modes when Vid is matched Experimental Results.

V. Results and Analysis

We have implemented system which enables to draw-wireless sensor network on Jpanel as shown in figure. Edges in the network represent wireless connectivity in nodes.

System enables user to

1) Distribute the keys to all nodes in the network

2) Select sensor node and base station

3) Send data

4) Setting forgery attacker

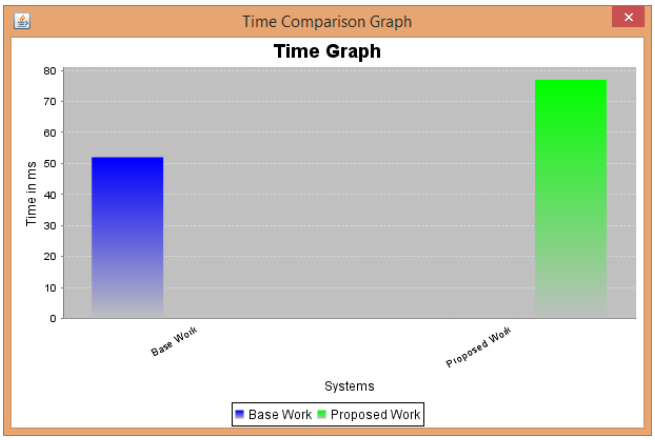
5) Create new network

Existing System and Proposed System are compared on two measures.

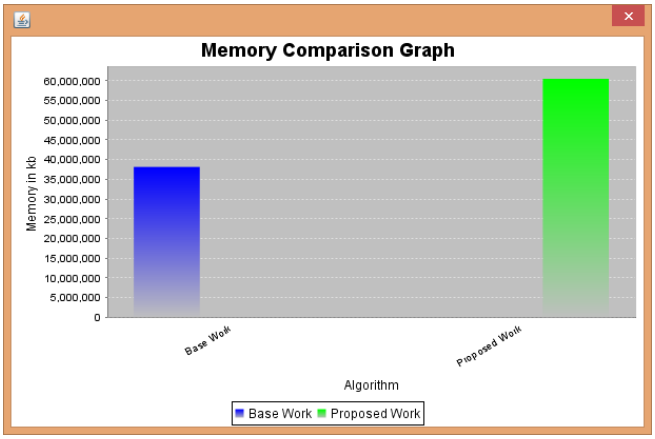
1) Time requirement to send the data from source to destination in milliseconds
2) Memory requirement to send data from source to destination in kilobytes

Table 1: Time Requirement and Memory Requirement

Requirement	Existing System	Proposed System
Time requirement in ms	52	77
Memory Requirement in kb	38	60



Graph 1: Time requirement comparison



Graph 2: Memory requirement comparison

From above results, it is clear that as per expectation proposed system is taking more time and memory for sending sensed data from source to destination but providing important feature to detect the forgery attacker from the network.

VI. Conclusion

This paper discussed various types for data provenance forgery detection. We described the need of provenance data for data transmitted in the network and the need of securing this provenance data. Approaches proposed in the literature for securing the provenance data are summarized. Most recent work [9] is based on securing provenance data against forgery attack and packet drop attack but it cannot identify the attacker. Proposed system resolved these issues and identifies the attacker. System uses bloom filter which makes detection and identification of provenance forgery lightweight so it is suitable for wireless sensor network. Proposed work detects and identity the attacker, so it will be very important information for prevention of such attacks.

REFERENCES

[1] A. Ramachandran, K. Bhandankar, M. Tariq, And N. Feamster,"Packets With Provenance," Technical Report Gt-Cs-08-02, Georgia Tech, 2008

[2] 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.

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

[6] 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.

[7] S. Sultana, M. Shehab, and E. Bertino, "Secure Provenance Transmission for Streaming Data," IEEE Trans. Knowledge and Data Eng., vol. 25, no. 8, pp. 1890-1903, Aug. 2013.

[8] Christian Esteve, Rothenberg and Carlos Macapuna, Alexander Wiesmaier," In-packet Bloom filters:Design and networking applications," 2009

[9] Salmin Sultana, Gabriel, Ghinita Elisa Bertino , Mohamed Shehab "A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks," IEE Trans. Dependable and Secure Comp., vol. 12, no. 3, 2015

Ashutosh Bajpei received his Bachelor's degree in Computer Engineering from Vidyavardhini's college of engineering and technology, Vasai Rd, Vasai Dist: Thane Now, he is pursuing his M.E degree in Computer Engineering from Sinhgad institute of technology, Lonavala, Pune University, Pune, India.His research areas are networking.

Prof Geetika Narang currently working Asst. prof at Sinhgad Institute of Technology, Lonavala B.E (CSE), Tech (CS).Subeditor of JAES, STES (Journal of Advance Engineering Science).Her Research Area: Wireless Sensor Network.