RESEARCH ARTICLE OPEN ACCESS

An insight on Provenance based detection of Packet Drop Attack and Data Forgery

Rohit D. Hedau[1], Dr. Pankaj Agrawal [2]
1(Department of Electronics and Comm. Engg / G. H. R.A.E.T., Nagpur)
2 (Department of Electronics and Comm. Engg / G. H. R.A.E.T., Nagpur)

Abstract:

The wireless sensor network (WSN) generates the data and forward it to intermediate nodes ,which finally forwards the data to the base stations(BS). The sensor nodes are prone introduction of malicious nodes by potential adversaries and it is necessary to address confidentiality, integrity and originality of data provenance. Data provenance allows the BS to trace the source and the forwarding path of an individual data packet. This work presents a brief survey on node level data provenance (which encodes history of data at each node) and the different techniques in WSN like in-packet-bloom filter, arithmetic coding and dictionary based provenance that make use of a light weight provenance scheme for detecting data forgery and packet drop attack.

I. INTRODUCTION

Wireless sensor networks are composed of low cost sensing devices with limited memory , computational and communication resources and limited batteries. They provides low-cost solutions in the applications such as battle-field surveillance, target tracking, environmental and health care monitoring, wildfire detection, traffic regulation etc. Thus the WSN are prone to many types of security attacks such as packet drop attack, false data injection and data forgery and eavesdropping.

This gives a brief survey on two of the major security attacks in WSN Packet drop attack and data forgery. A genuine problem is to confirm whether a packet loss(due to overload in network) or Packet drop(malicious node dropping it) or packet drop attack (i.e. Selective packet drop attack by malicious node which causes messages not to reach the intended destination hence required action may not happen). Data forgery detection is essential as the information moving within the WSN carries critical information used for taking necessary decisions. Hence assuring trustworthiness of data is necessary that checks whether the data has been modified along its path which may result Base Station to take wrong decisions.

II. DETAILS OF PROVENANCE

Provenance at base is a technique used to trace out the history of an object. Provenance carries information like the history of data such as its place of origin, creator/publisher of data, creation date, modifier or modification date etc. . The actual meaning of provenance depends on the application on which it is applied. In WSN provenance includes the origin of data packet, how it is processed through multiple intermediate nodes and its traversal in a network to reach the destination BS.

2.1 SENSOR NETWORK AND PROVENANCE

In WSN provenance holds the history of data such as source node information and complete route information. Source node information includes information as to from where the packet originated and complete route information includes the path the data packet traversed form source node to BS. Each data packet contains: (i) a unique sequence number (ii) source node information (iii) data value (iv) provenance and (v) message authentication code (MAC).

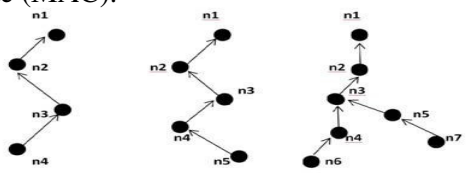

Fig -1: Provenance graphs of sensor networks

According to ChangdaWang[20] provenance is stated as Given a data packet d, the provenance p_d is a directed acyclic graph G(V,E) satisfying the following properties:

- P_d is a subgraph of the sensor network G(N,L).
-
- forv_x,v_y in V , v_y is a child of v_x if and only if HOST(v_y) forwards d to HOST(v_x).

Where V-Vertex, E-Edges , N-Network, L-Link .

Provenance transmission in Wireless Sensor Networks supports data transmission with non-negligible energy usage. In a multi-hop network, provenance includes knowledge of the originator and processing path of data since its generation. Thus, every intermediate node is ready with provenance of hop count between that node and the originator of the data item.
Provenance is complex and need a large variable to represent it and dissipates high energy. Chuang Wang et al[20] Proposes an energy-efficient provenance encoding and construction scheme known as Probabilistic
Provenance Flow (PPF). The paper also demonstrates the feasibility of adapting the Probabilistic Packet Marking (PPM) technique in IP trace back in wireless sensor networks
Provenance has to be managed while keeping high throughput, low bandwidth consumption, storage efficiency and secure transmission. Mohamed Shehab et al[19] discusses a new approach to securely transmit provenance for streaming data by embedding provenance into the inter-packet timing domain. The challenge here is, with the increasing size of provenance, it should still be able to effectively manage and minimize the additional bandwidth consumption.

.

III. DISCUSSION ON PACKET DROP ATTACK

Detecting Malicious Packet Losses is a big challenge because normal network at congestion appear to do the same. Present day networks drop packets above their processing and storing capabilities. Some of the existing detection protocols have tried to address this problem with a user-defined threshold. One of the techniques uses a compromised router detection protocol that measures the traffic rates, buffer sizes and the number of congestive packet losses that occur. Using this information, the ambiguity is removed and subsequent packet losses are detected as malicious packet loss.

Taiwan et al[1] discusses the various negative impacts of packet dropping attacks that are as mentioned:
Delay: Retransmissions increases the file transfer time.
Response time: Dropping DNS query keeps the user idle for a long time to get a web page.
Quality: Dropping some packets degrades the quality of the service.
Bandwidth: packets dropped leads to retransmissions affecting bandwidth.

3.1 PACKET DROPPING ATTACK DETECTION TECHNIQUES

Kennedy Edemacu et al [2] propose several techniques to deal with the packet drop attack:
(i)Watch Dog Technique: In this technique, every node acts as a watchdog agent monitoring packet transmissions to neighboring nodes..

(ii)Side Channel Monitoring (SCM) : In SCM a sub-set of neighbors for each node in a route between source and destination are selected to keep track of their message forwarding behaviors

(iii)Monitoring Agent Technique: The technique is based on capturing packets sent by neighboring nodes within a transmission range with all nodes collecting information about their one hop neighbors within a certain period of time

(iv)PathRater: In this technique a PathRater is run by every node in the network which maintains ratings for every other node A path metric is calculated by averaging the ratings for nodes in the path

According to V. Bhuse et al[3] the existing techniques to detect packet drop attack needs vigil on all the nodes in the network . Once malicious nodes that drop packets are detected, a new path has to be found that does not include them. The paper proposes a lightweight solution
called DPDSN which identifies the paths that drop packets by using alternate paths, these alternate paths are the paths that WSN finds earlier during route discovery.

Chuang Wang et al[4] proposes a simple yet effective scheme called as Probabilistic Nested Marking (PNM) that recognizes the misbehaving forwarders who drop or modify packets. The scheme identifies packet modifiers with a certain probability. In PNM, a dynamic routing tree rooted at the BS is first established, when sensor data is transmitted along the tree structure towards the BS, each packet sender or forwarder adds a small number of extra bits, which is called packet marks, to the packet Once the information of node behaviors has been collected, the BS uses the heuristic ranking algorithm to identify the most likely bad nodes from the suspiciously bad nodes.

N. Vanitha et al[5] proposes a node categorization algorithm that recognizes which sensor node is the actual packet dropper. The algorithm also distinguishes the actual packet dropper from suspicious packet dropper. Identifying the actual packet dropper is a 3-step process that includes:

(1)Initialization Phase :

(2)Categorization Phase:

(3)Detection Phase:
Salmin sultana et al[5] proposes that detection of malicious node involves 3 phases (i) Detecting Packet Loss (ii) Identification of Attack Presence (iii) Localizing the Malicious Node/Link.
The presence of packet loss is detected by checking inter-packet delays. To locate a malicious node, other than Node-ID, time stamp, hash value of the data etc. are added to the provenance. provenance and detects the malicious node that drop packet in that path.

IV. DISCUSSION ON DATA FORGERY ATTACKS

Any malicious sensor node in network can inject false data during both data aggregation and data forwarding. Some of the existing techniques prevent false data injections during data forwarding by not allowing the forwarding node to modify the data packet.
GaragaSubba Rao et al[8] proposes a technique that prevent false data injections during both data forwarding and data aggregation using DSP(Dynamic Security Protocol). Traditional symmetric key cryptography algorithms, does not achieve both end-to-end confidentiality and network data aggregation. The proposed technique in not an energy efficient way of performing secure data aggregation and suffers from delays.

S. N. Saranya et al[7] proposes a Statistical En-route Filtering mechanism (SEF) technique that prevents single compromised node from breaking down the entire system. This technique carefully rations the amount of security information percolated to any single node .

V. PROVENANCE BASED PACKET DROP ATTACK AND FORGERY DETECTION

5.1 TECHNIQUE BASED ON BLOOM FILTER

In-packet Bloom-filter[10] is technique used for provenance encoding. Provenance provides historical data of nodes and the size of data goes on increasing with the increase in the number of nodes, which turns out to be inefficient . The basic focus is make provenance light weight which results decrease in the dissipated energy. The alternate focus is to design a provenance encoding and decoding mechanism that satisfies security and performance parameters .

The bloom filter decides the size of Provenance. The Bloom filter stores provenance . Initially bloom filter is set to zero. With every hop Vid(vertex id) is generated at each node and the filter is set to 1. This technique uses node level provenance which encodes the provenance at each node that are involved in each step of packet path. The Compression or encoding technique ensures that the system does not lose any provenance information after decoding.

5.2 TECHNIQUE BASED ARITHMETIC CODING

Arithmetic coding is employed for data compression with an advantage of reduced provenanceand proves out to be a technique which removes most of the disadvantages of previous techniques. Hussain et al[20] discusses that provenance size is not directly proportional to the number of hops, but to the occurrence probabilities of the nodes that are on a packet's path. Other schemes drop op critical information while compressing provenance record and do not include the edges that indicate directed connections among sensor nodes and thus fail to provide accurate packet path topologies.

5.3 DICTIONARY BASED PROVENANCE

Changda Wang et al[21] proposes a dictionary based provenance approach that makes provenance size completely independent of number nodes in the network. The provenance size is independent of hop count hence gives high utilization of bandwidth and less energy consumption. In dictionary based secure provenance scheme each sensor node in the network stores a packet path dictionary(PPD) . Using PPD, instead of entire path a path index is enclosed with each packet. Since the packet path index is a code word of a dictionary, its size is independent of the number of nodes present in the packet's path.

VI. CONCLUSIONS

This paper is a brief survey on major security attacks and its impact on network. The paper discusses on two major security attacks packet drop attack and data forgery. Several existing technique to detect these two attacks and their disadvantage discussed. After a brief survey on provenance and its application in network, it is analyzed that use of light weight provenance scheme for detection of packet drop attack and data forgery in wireless sensor network yields better bandwidth utilization

ACKNOWLEDGMENT

The authors are thankful to the college authorities for providing the necessary technical assistance in terms of laboratory, software tools and supervisors to carry on with the research work .

REFERENCES

[1]. Xiaobing Zhang S. F. Wu ;Zhi Fu ; Tsung-Li Wu "Malicious Packet Dropping: How It Might Impact the TCP Performance and How We Can Detect It",pages.263-270,2000.

[2]. Kennedy Edemacu , Martin Euku and Richard Ssekibuule ,"Packet Drop Attack Detection Techniques In Wireless Ad Hoc Networks" ,vol.6,September 2014.

[3].V. Bhuse, A. Gupta, and L. Lilien, "DPDSN: Detection of Packet-Dropping attacks for Wireless Sensor Networks

[4]. Chuang Wang, Taiming Feng, Jinsook Kim, Guiling Wang, and Wensheng Zhang ," Catching Packet Droppers and Modifiers in Wireless Sensor Networks",vol.23,issue-5,pages.835-843,April 2011

[5]. N. Vanitha, G.Jenifa," Detection of Packet Droppers in Wireless Sensor Networks Using Node Categorization Algorithm".

[6] Salmin sultana ,Elisa bertino, Mohamed Shehab "A Provenance based Mechanism to Identify Malicious Packet Dropping Adversaries in Sensor Networks",pages.332-338,2011

[7]. M. Tharani, K. Sivachandran, S. N. Saranya, " An Efficient Detection Of Forgery And Packet Drop Attacks In Wireless Sensor Networks",vol.2,issue-7,Nov-2015.

[8]. GaragaSubba Rao, Kothapalli Ramesh, "False Data Detection in Wireless Network using Dynamic Security Protocol",vol.3,pages.4718-4722,2012.

[9]. S. Sultana, G. Ghinita, E. Bertino, and M. Shehab, "A lightweight secure provenance scheme for wireless sensor networks," in 2012 IEEE 18th International Conference on Parallel and Distributed Systems (ICPADS), 2012, pp. 101–108

[10]. S. Sultana, G. Ghinita, E. Bertino, and M. 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. 99, no. PrePrints, p. 1, 2014.

[11]. I. H. Witten, R. M. Neal, and J. G. Cleary, "Arithmetic coding for data compression," ACM, vol. 30, no. 6, pp. 520–540, 1987.

[12]. Hussain , Syed Rafiul , Wang, Changda, Sultana, Salmin , and Bertino, Elisa, "Secure Data Provenance Compression Using Arithmetic Coding in Wireless Sensor Networks" (2014).Cyber Center Publications.Paper 645.

[13].*Wang Changda ,Hussain S and Bertino E "Dictionary based secure provenance compression for wireless sensor network ", ISSN:1045-9219, 2015 ,Volume:pp , Isssue:99.*