A Provenance Mechanism to Identify Malicious and Packet Drop Attacks in Wireless Sensor Networks

Ms. R. Shakila
M.E., CSE
University College of Engineering, Tiruchirappalli
Tiruchirappalli, India

Ms. R. Renuga Devi
Teaching Fellow, Dept of IT
University College of Engineering, Tiruchirappalli
Tiruchirappalli, India

***Abstract*—In Wireless Sensor Network data flow from multiple sources through intermediate processing node that gather information. A malicious user could introduce additional nodes within the network or compromise existing ones. Therefore, reassuring high information trustiness is crucial for proper decision-making. Data provenance represents several schemes such as provenance encoding and provenance decoding scheme. Using these schemes the system can detect the packet loss attack and provenance fraud. Provenance encoding scheme uses the stable Bloom filters to encode provenance. A malicious may perform traffic anywhere on the path to modify the packet so that this approach uses provenance verification and collection to encode the packet and this method introduces a data aggregation mechanism at the base station. Provenance verification will be conducts in the base station the verification process not only to verify its knowledge of provenance but also to check the rectitude of the transmitted provenance. If the verification fails then the failed process send to provenance collection part. This system can easily notify the malicious node in the network. The objective is to achieve the security properties such as Confidentiality, rectitude and Freshness.**

Keywords*— *Wi-fi Sensor community, protection, Provenance, stable Bloom Filter

INTRODUCTION

A wireless detector network is distributed autonomous sensors to look at environmental conditions, like temperature, sound, pressure, etc. and at hand in glove pass their data through the network to a main location. and to hand in glove pass their knowledge through the network to a main location. One of the main issues in WSN is malicious nodes spoofing their identity and location. A packet drop attack or part attack may be a style of denial-of-service attack during which a router that's alleged to relay packets instead discards them. This sometimes happens from a router changing into compromised from variety of various causes. One cause is thru a denial-of-service attack on the router employing a famed DoS tool. Sensor networks are used in numerous utility domains, equivalent to cyber physical infrastructure systems, environmental monitoring and energy grids. Information are produced at a giant number of sensor node sources and processed in network at intermediate hops community on their approach to a Base station that performs selection-making. The diversity of information sources create the need to assure the trustworthiness of knowledge to simplest dependable expertise is viewed in the selection system.

The packet drop attack will be oftentimes deployed to attack wireless networks. Because wireless networks have a far totally different design than that of a typical wired network, a bunch will broadcast that it's the shortest path towards a destination. By doing this, all traffic are directed to the host that has been compromised, and therefore the host is ready to drop packets at can. Also over a wireless device network, hosts square measure specifically liable to cooperative attacks wherever multiple hosts can become compromised and deceive the opposite hosts on the network. In a wireless sensor network, data provenance allows for the BS to trace the supply and forwarding course of character information packets.

Provenance ought to be recorded for every packet. However primary challenges arise as a result of the tight storage, energy and bandwidth constraint of sensor nodes. As a consequence, it's indispensable to devise a mild-weight provenance answer with low overhead. As a result it's crucial to address protection requisites like confidentiality, rectitude and freshness of provenance. This system predominant goal is to design a provenance encoding and decoding process that satisfies security and performance need.

System suggests a provenance encoding procedure whereby each node on the trail of an information packet securely embeds provenance information inside a Bloom filter that is transmitted along with the info. Upon receiving the packet, the bottom station extracts and verifies the provenance information. This system also devise an extension of the provenance encoding scheme that makes it possible for the bottom station to discover if a packet drop assault used to be staged by a malicious node.

In wireless device networks, malicious could launch some attacks attributable to packet dropping so as to disrupt the communication. To tolerate or avoid such attacks, some of the schemes have been proposed. But only a few will effectively and with efficiency determine the malicious. This method is simple and so identifies the forwarders that drop the packets.

Wireless sensor network is most needed and operated in environment to monitor events, produce and transmit data. Data's in the sensor network could be a transferred by gateway, base station, storage node, or querying user. Wireless sensors networks is used in major applications in Military and defence networks. When it's deployed in such associate degree atmosphere, it lacks physical protection and is subject to node compromise. After compromising one or multiple sensor nodes, a malicious may launch various attacks to disrupt the inter-network communication.

One of the attacks is packet drop attack, wherever a compromised node drops packets maliciously within the path. Several techniques are planned to sight the packet drop attack in wireless sensing element networks.Detecting malicious packet dropping is very important in Wireless sensing element networks, security attacks like blackhole, greyhole, and hollow attacks.

Section II describes background. The details of secure birthplace secret writing and secret writing is given in Section III implementation and connected add Section IV.

II. BACKGROUND

A. Network Model

This procedure has to create a multihop wi-fi sensor network, inclusive of a multiple quantity of sensor nodes and a base station that collects knowledge from the source. There exists a base station (BS) that acts as root and connects the community to infrastructures such as the internet.

B. Data Model

The sensor network helps a couple of distinguishable knowledge flows the place supply nodes generate information periodically. A node may additionally obtain data from other nodes with a view to forward them toward the BS. Each knowledge packet involves of (i) a particular packet sequence quantity, (ii) a knowledge value, and (iii) provenance.

C. Stable Bloom Filter (SBF)

Stable bloom filter is variant of bloom filter which might be accustomed notice duplicates in data-stream. Due to the fact that there is no strategy to retailer entire history of data circulation, so stable bloom filter makes use of extra up to date elements to search out duplicates. SBF continuously evicts the stale understanding so that SBF has room for those extra contemporary factors.

D. Adversary model

Throughout the network operations, every node however the BS could also be compromised through adversaries. An adversary can eavesdrop within the network and accumulate exclusive expertise by means of packet sniffing, site visitors analysis and so forth. Our objective is to achieve the next safety homes:

• Confidentiality: An adversary cannot be taught any understanding about information provenance by examining the contents of the packet.

• Integrity: (i) an adversary are not able to inject counterfeit knowledge within the provenance or cast off any benign node.

(ii) A malicious node cannot drop packets without being recognized.

• Freshness: Packet replay assaults are detectable.

III. IMPLEMENTATION

A. Provenance Encoding

AES algorithm to encode the info for the information protection. For a packet, provenance encoding refers to propagating the vertices within the provenance graph and inserting them into the stable bloom filter. Every vertex originates at a node in the information route and represents the provenance document of the host node. A vertex is uniquely recognized via the vertex id (VID). The provenance document of a node entails 1) the node id, and 2) an acknowledgement of the lastly located packet in the flow.

B. Provenance Decoding

When a Base station receives a knowledge packet Base station is aware of what the info packet should be assessments. Afterwards, upon receiving packets, it is sufficient for the BS to verify its skills of provenance with that encoded within the packets. In provenance decoding it conducts two procedure particularly provenance verification and provenance collection.

Algorithm-1 Provenance Verification:
Input: Received packet with sequence seq and SBF sbf. Set of hash functions H, Data path P=<n l 1,…,n1,….,np> SBFc ← 0 // Initialize Stable Bloom Filter
For each ni ∈ P do
Vid I = generate VID (n i, seq)
insert vid I into SBFc using hash functions in H endfor
if (SBF c = sbf) then
return true // Provenance is verified endif
return false

Algorithm-2 Provenance Collection:
Input: Received packet with sequence seq and SBF sbf. N Set of nodes (N) in the network, Set of hash functions H
1. Initialize
Set of Possible Nodes S ← ∅
Stable Bloom Filter SBF c ← 0 // to represent S
2. Determine possible nodes in the path and build the representative SBF

for each node n i ∈ N do
vid i = generateVID (n i
, seq) if (vid i is in sbf)
then
S ← S ∪ n i
insert vid i into SBF c using hash functions in
H endif
endfor
3. Verify SBF c with the
received SBF if (SBF c = sbf)
then
return S // Provenance has been determined
correctly else
return NULL // Indicates an in-transit
attack endif

C. Detecting Provenance Forgery

The verifier before storing the data packet on the destination preprocesses the information packet and appends some Meta data to the packet and outlets at the destination. At the time of verification the verifier uses this Meta data to affirm the rectitude of the information. It's most important to note that our proof of knowledge rectitude protocol just tests the rectitude of information i.E. If the info has been illegally modified or deleted. It may be avert the destination from modifying the info.

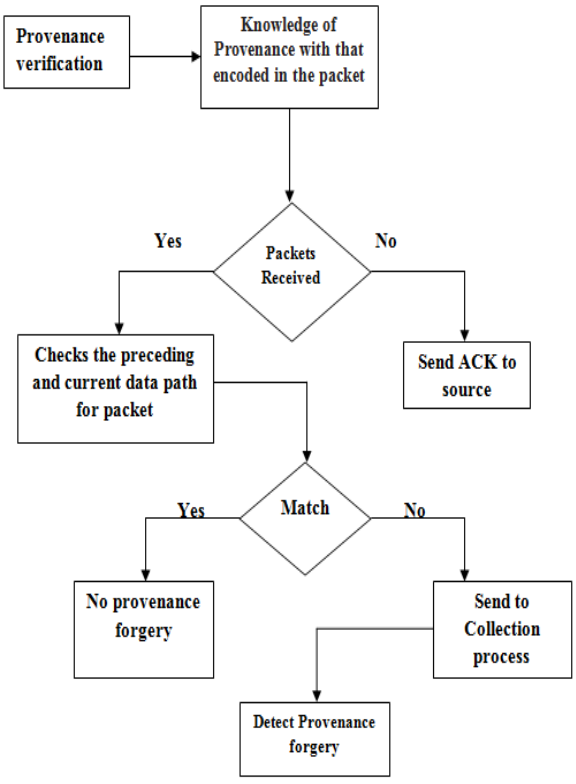

Figure2: Detecting Provenance Forgery

V. RELATED WORK

A lightweight secure provenance scheme situated on in-packet Bloom filter. On this procedure, all nodes on a packet's course are embedded in the BF making use of a collection of hash capabilities. Upon receiving a packet, the BS retrieves the nodes on the trail with a certain false constructive cost. Such false optimistic cost relies on the size of the BF. The bigger the BF measurement is, the lower the false positive charges are. SBF is better in terms of accuracy and time when unique quantity of FP rates are applicable and the gap is slightly small, which is the case in many data circulate applications as a result of the actual-time constraint. When the space is fairly massive or most effective tiny FP charges are allowed, buffering is best. AES algorithm which dynamically updates the sketch to symbolize contemporary information. We find and show the stable residences of an SBF together with stability, exponential convergence fee and monotonicity, founded on which we show that using regular space, the danger of a false constructive can also be bounded to a regular independent of the move dimension, and this consistent is explicitly derived.

Data Provenance

Data provenance is a foremost role for assuring information trustworthiness. In a multi-hop sensor community, knowledge provenance permits the bottom station to trace the source and forwarding sensor nodes of a character d*ata* packet seeing that its iteration. To make certain information exceptional and trustworthiness, it is vital to document the provenance of each and every information packet, together with understanding about every node within the information float path. Nevertheless, vigour and bandwidth barriers, tight storage, and useful resource constraints of sensor nodes make the gathering of data provenance difficult.

VI. CONCLUSION

The proposed system has addressed the main issue of securely transmitting provenance for sensor networks, and proposed a soft-weight provenance encoding and decoding scheme founded on stable Bloom filters. The scheme ensures confidentiality, rectitude and freshness of provenance. Procedure increased the scheme to incorporate information-provenance binding, and to include packet sequence expertise that supports detection of packet loss assaults. This project contributed one method, sharing the packet with secret that's the bottom line is generated by means of the node. The secrets and techniques are positions where embed with provenance. The node encrypts the secrets making use of the key for personal utilization and the proposed approach uses the AES algorithm for packet encryption. The developed Encryption general (AES) specifies a FIPS-accredited cryptographic algorithm that can be used to safeguard digital knowledge. The AES algorithm is a symmetric block

cipher that may encrypt (encipher) and decrypt (decipher) knowledge of the packets. Encryption converts knowledge to an unintelligible form known as cipher text; decrypting the cipher textual content converts the data again into its normal type, referred to as plaintext the packets might be shared on a base station. In this method key replacing, cryptography, and signature method are used. So with no trouble realize the suspicious data. The verify module used to realize the suspicious data and provenance information of the node.

REFERENCES

[1] S. Sultana, G. Ghinita, E. Bertino, "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, pp no. 256-269 May/June 2015

[2] H. Lim, Y. Moon, and E. Bertino, "Provenance-Based Trustworthiness Assessment in Sensor Networks," Proc. Seventh Int'l Workshop Data Management for Sensor Networks, Vol. 7, pp. 2-7, 2010.

[3] K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, "Provenance-Aware Storage systems," Proc. USENIX Ann. Technical Conf., Vol. 5,pp. 4-4, 2006.

[4] 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, Vol. 16, pp. 332- 338, 2011.

[5] A. Kirsch andM. Mitzenmacher, "Distance-Sensitive BloomFilters," Proc.Workshop Algorithm Eng. and Experiments, Vol. 3, pp. 41-50, 2006.

[6] C. Rothenberg, C.Macapuna,M.Magalhaes, F. Verdi, and A. Wiesmaier, "In-Packet Bloom Filters: Design and Networking Applications," Computer Networks, vol. 55, no. 6, pp. 1364-1378, 2011.

[7] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. Int'l Workshop Sensor Network Protocols and Applications, Vol. 2, pp. 113-127, 2003.

[8] M. Mitzenmacher, "Compressed Bloom Filters," Proc. ACM Symp. Principles of Distributed Computing, Vol. 20, pp. 144-150, 2001.

[9] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-Route Filtering of Injected False Data in Sensor Networks," Proc. IEEE INFOCOM, Vol. 13, pp. 839-850, 2004.

[10] 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.

[11] A. Ghani and P. Nikander, "Secure In-Packet Bloom Filter Forwarding on the Netfpga," Proc. European NetFPGA Developers Workshop, Vol. 11, pp. 25-31 2010.