International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 23 Issue 8 –NOVEMBER 2016.

PACKET DROP, FORGERY ATTACK AND DETECTION METHODS IN WIRELESS SENSOR NETWORK

NATTA PAVANI [#1], V.PADMAJA [*2] and SAYEED YASIN[*3]

[#] *Student, M.Tech (C.S.E), Nimra College of Engineering & Technology, A.P., India.*

[*2] *Assistant professor , Dept. of Computer Science & Engineering, Nimra College of Engineering & Technology, A.P., India.*

[*3]*Associate professor & Head, Dept. of Computer Science & Engineering, Nimra College of Engineering & Technology, A.P., India.*

***Abstract*— Sensor networks are used in application domains such as cyber physical communications, ecological checking, whether monitoring power grids, etc. The data that should be large sensor node sources and processed in-network with their way to a Base Station (BS) that performs which decision should be taking. Data are flowed from various sources through transitional processing nodes that aggregate information and cruel opposition may introduce extra nodes in the network or compromise existing ones, assuring high data trustworthiness is crucial for correct decision-making. There are many promising attacks like provenance forgery, Packet drop attack, DDos attack, Jamming attack etc. are found in the WSN while transmitting the data. A malicious adversary may introduce additional nodes in the network or compromise existing ones. Therefore, assuring high data trustworthiness is crucial for correct decision-making. Data provenance keeps log information of data about who accessed this data, who modified this data, the path from the data is traversed etc. Data provenance has important role in the evaluation of trustworthiness of data therefore, it is important to secure data provenance. The packet drop attack can be frequently deployed to attack wireless sensor network. The malicious router can also accomplish this attack selectively. The several challenging requirements for provenance management and packet drop attacks in sensor networks are low energy and low bandwidth consumption, competent storage and secure transmission. We evaluate the proposed technique both analytically and empirically, and the results prove the effectiveness and efficiency of the lightweight secure provenance scheme in detecting packet forgery and loss attacks.**

Index Terms*— *Wireless sensor network, Provenance forgery attack, Packet Drop attack.

I. INTRODUCTION

Sensor networks are used in application domains such as cyber physical communications, ecological checking, whether monitoring power grids, etc. The data that should be large sensor node sources and processed in-network with their way to a Base Station (BS) that performs which decision should be taking. Information is considered in the decision process or making. Data provenance is an effective method to assess data trustworthiness, and the actions performed on the data. Provenance in sensor networks has not been present properly addressed. Investigate the problem of secure and efficient provenance transmission and handling for sensor networks, and we use origin to detect packet failure attacks dramatic by cruel sensor nodes. In a multi-hop sensor network, data origin allows the BS to trace the source and forwarding path of an individual data packet. Origin must be witnessed for each packet, but important tests arise due to the tight storage, energy and bandwidth of sensor nodes. More sensors often operate in an untrusted environment, it may be subject to show aggressions. To address the security such as confidentiality, integrity and freshness of provenance. Propose a provenance encoding strategy for each node on the data packet securely embeds provenance data with a Bloom filter (BF) that is transmitted along with the data. Upon on receiving the packet, the BS extracts and prove the provenance information. To extend the provenance encoding scheme allows the BS to detect packet drop attacks during the sensor node transmission. In the existing research that employs separate transmission channels for data provenance, it only requires a single channel for both. Usual origin security solutions use seriously cryptography and digital signatures and they employ appended based data structures to store provenance, leading to prohibit costs. Use message authentication code (MAC) schemes and Bloom filter, which are fixed-size data structures that compactly represent provenance. In a wireless sensor network, data are produced at a large number of sensor node sources and processed in network at intermediate hops network on their way to a Base Station that performs decision-making. The diversity of data sources create the need to assure the trustworthiness of data such as only trustworthy information is considered in the decision process. Sensor nodes monitor the environment, detect events of interest, produce data and collaborate in forwarding the data towards a sink, which could be a gateway, base station, storage node, or querying user. A sensor network is often deployed in an unattended and hostile environment to perform the monitoring and data collection tasks. When it is

deployed in such an environment, it lacks physical protection and is subject to node compromise. After compromising one or multiple sensor nodes, an adversary may launch various attacks to disrupt the in-network communication. In a multi-hops sensor network and data provenance allows the BS to trace the source and forwarding 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 constraint of sensor nodes. Therefore, it is necessary to devise a light-weight provenance solution with low overhead. Hence it's necessary to address security requirements like confidentiality, integrity and freshness of provenance. Our important goal is to design a provenance encoding and decoding method that satisfies security and performance need. To deal with packet droppers, a broadly adopted countermeasure is multi-path forwarding in which each packet is forwarded along multiple redundant paths and hence packet dropping in some but not all of these paths can be tolerated. This scheme introduces high extra communication overhead.

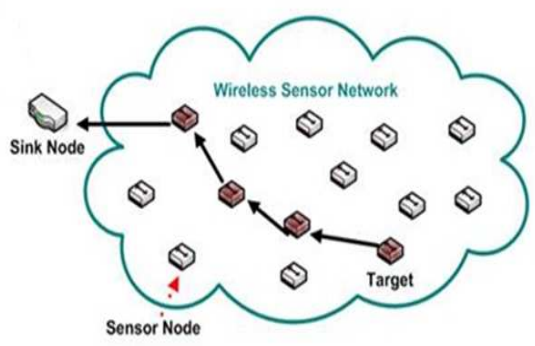

Figure 1: System Model

II. PROPOSED SYSTEM:

In this paper, we propose We investigate the problem of secure and efficient provenance transmission and processing for sensor networks, and we use provenance to detect packet loss attacks staged by malicious sensor nodes.

Our goal is to design a provenance encoding and decoding mechanism that satisfies such security and performance needs. We propose a provenance encoding strategy whereby each node on the path of a data packet securely embeds provenance information within a Bloom filter (BF) that is transmitted along with the data. Upon receiving the packet, the BS extracts and verifies the provenance information. We 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 node.

A. ADVANTAGES OF PROPOSED SYSTEM:

We use only fast message authentication code (MAC) schemes and Bloom filters, which are fixed-size data structures that compactly represent provenance. Bloom filters make efficient usage of bandwidth, and they yield low error rates in practice.

We formulate the problem of secure provenance transmission in sensor networks, and identify the challenges specific to this context.

We propose an in-packet Bloom filter (iBF) provenance-encoding scheme.

We design efficient techniques for provenance decoding and verification at the base station.

We extend the secure provenance encoding scheme and devise a mechanism that detects packet drop attacks staged by malicious forwarding sensor nodes.

We perform a detailed security analysis and performance evaluation of the proposed provenance encoding scheme and packet loss detection mechanism.

We only require a single channel for both transmission channels for data and provenance.

III. LITERATURE SURVEY

Data are produced at a large number of sensor node sources and processed in-network at intermediate hops on their way to a base station that performs decision-making. The diversity of data sources creates the need to assure the trustworthiness of data. Data provenance is an effective method to assess data trustworthiness. [1] focused on the problem of secure provenance transmission in sensor networks, and identify the challenges specific to this context by implementing Message Authentication Code (MAC) schemes and Bloom filters and perform a detailed security analysis and performance evaluation of the proposed provenance encoding scheme and packet loss detection mechanism by representing unique sequence number per packet and provenance encoding and decoding at the base station.

A sensor network is often deployed in an unattended and hostile environment to perform the monitoring and data collection tasks. When it is deployed in such an environment, it lacks physical protection and is subject to node compromise. After compromising one or multiple sensor nodes, an adversary may launch various attacks to disrupt the in-network communication. Among these attacks, two common ones are dropping packets and modifying packets, i.e., compromised nodes drop or modify the packets that they are supposed to forward. To identify the Packet Droppers and Packet Modifiers [2] ranking algorithms and packet marks were used. The Performance is represented using detection rate and false positive probability. The Proposed scheme provides an effective mechanism for catching compromised node.

Packet dropping and modification are common attacks that can be launched by an adversary to disrupt communication in wireless multi-hop sensor networks. A simple yet effective scheme is used which can identify misbehaving forwarders that drop or modify packets. According to the scheme, a dynamic routing tree rooted at the sink is first established. When sensor data is transmitted along the tree structure towards the sink, each packet sender or forwarder adds a small number of extra bits, which is called packet marks [3], to the packet. Based on the packet marks, the sink can figure out the dropping rate associated with every sensor node. Node Categorization Algorithm used to identify nodes that are droppers/modifiers for sure or are suspicious droppers/modifiers.

MANETs have become a commonly used network for

various applications. But this advantage suffers with serious security concerns, mainly a wireless transmission medium perspective where such networks may be subject to packet dropping. Mobility and portable nature of Mobile Ad hoc Network may also lead to link failure. During packet forward, valuable packets may be dropped by malicious nodes present in the network. Link error and malicious packet dropping are the two sources for packet losses in MANET. [4] Introduces a new protocol named secured Ad hoc on demand distance vector (SAODV), which can truthfully detect packet dropping attack in MANET. SAODV can detect malicious nodes by identifying dropping of routing and data packet. Packet dropping due to both link error and presence of malicious nodes can detect by SAODV. It also provides importance to preserve privacy of data.

IV. RELATED WORK

A. *Detect Attack Module:*

Differs from the received iBF, it indicates either a change in the data flow path or a BF modification attack. The verification failure triggers the provenance collection process which attempts to retrieve the nodes from the encoded provenance and also to distinguish between the events of a path change and an attack. Such an inference might introduce errors because of false positives If the verification succeeds, decide that there was a natural change in the data path and have been able to determine the path correctly. Otherwise, an attack has occurred. If the data aggregation result is verified at the BS, then the data provenance coupling is ensured at each node in the routing path. Against attacks the précis diffusion and Lightweight verification algorithm to verify at BS if the computed overall is correct. This algorithm is user to sense packet drop from cruel nodes. The BS computes the final synopsis using the messages from its child nodes and verifies the received MACs.

B. *Encode provenance Security:*

Each packet consists of a unique sequence number, data value, and an iBF which holds the provenance, focus is on securely transmitting provenance to the BS. In an aggregation infrastructure, securing the data values is also an important aspect, secure provenance technique can be used in conjunction with such work to obtain a entire solution that provides security for data, provenance and data-provenance binding. For a data packet, provenance encoding refers to generating the vertices in the provenance graph and inserting them into the iBF. Each vertex creates at a node in the data path and represents the provenance record of the host node. A vertex is uniquely identified by the vertex ID. The VID is generated per-packet based on the packet sequence number (seq) and the secret key Ki of the host node. We use a block cipher function to produce this VID in a secure manner. A Provenance encoding scheme whereby each node on the path of a data packet securely embeds provenance information .

C. *Detecting Packet Drop Attacks Mechanism*

We extend the secure provenance encoding scheme to detect packet drop attacks and to identify malicious node(s). We assume the links on the path exhibit natural packet loss and several adversarial nodes may exist on the path. For simplicity, we consider only linear data flow paths (i.e., as illustrated in Fig. 1(a)). Also, we do not address the issue of recovery once a malicious node is detected. Existing techniques that are orthogonal to our detection scheme can be used, which may initiate multipath routing [6] or build a dissemination tree around the compromised nodes [17]. We augment provenance encoding to use a packet acknowledgement that requires the sensors to transmit more meta-data. For a data packet, the provenance record generated by a node will now consist of the node ID and an acknowledgement in the form of a sequence number of the lastly seen (processed/forwarded) packet belongingto that data flow. If there is an intermediate packet drop, Some nodes on the path do not receive the packet. Hence,during the next round of packet transmission, there will bea mismatch between the acknowledgements generated fromdifferent nodes on the path. We utilize this fact to detectthe packet drop attack and to localize the malicious node.We consider a data flow path P where nlis the only datasource. We denote the link between nodes niand n(i+1)as li. We describe next packet representation, provenance encoding and decoding for detecting packet loss.

V. CONCLUSION AND FUTURE WORK

In this paper, We addressed the problem of securely transmitting provenance for sensor networks, and proposed a light-weight provenance encoding and decoding scheme based on Bloom filters. The scheme ensures confidentiality, integrity and freshness of provenance. We extended the scheme to incorporate data-provenance binding, and to include packet sequence information that supports detection of packet loss attacks. Experimental and analytical evaluation results show that the proposed scheme is effective, light-weight and scalable. In future work, we plan to 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] H. Lim, Y. Moon, and E. Bertino, “Provenance-based trustworthiness assessment in sensor networks,” in *Proc. of Data Management for Sensor Networks*, 2010, pp. 2–7.

[2] I. Foster, J. Vockler, M. Wilde, and Y. Zhao, “Chimera: A virtual data system for representing, querying, and automating data derivation,” in *Proc. of the Conf. on Scientific and Statistical Database Management*, 2002, pp. 37–46.

[3] K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, “Provenance-aware storage systems,” in *Proc. of the USENIX AnnualTechnical Conf.*, 2006, pp. 4–4.

[4] Y. Simmhan, B. Plale, and D. Gannon, “A survey of data provenance in e-science,” *SIGMOD Record*, vol. 34, pp. 31–36, 2005.

[5] R. Hasan, R. Sion, and M. Winslett, “The case of the fake picasso: Preventing history forgery with secure provenance,” in *Proc. Of FAST*, 2009, pp. 1–14.

[6] S. Madden, J. Franklin, J. Hellerstin, and W. Hong, "TAG: a tiny aggregation service for ad-hoc sensor networks," *SIGOPS Operating Systems Review*, no. SI, Dec. 2002.

Ms Natta Pavani is a student of NIMRA College of Engineering and Technology, IBRAHIMPATNAM,VIJAYAWADA. She is presently pursuing her M.Tech degree from JNTU,Kakinada.

V.PADMAJAIS presently working as Assistant professor in CSE department,NIMRACollege of Engineering and Technology, IBRAHIMPATNAM, Vijayawada.

SAYEED YASIN received his MTECH in Computer Science & Engg from JNTU Hyderabad. He is pursuing Ph.D., in Rayalaseema University, Kurnool. He is currently working as an Associate Professor & Head in Nimra College of Science & Technology the Department of Computers Science and Engineering & Technology, Jupudi, Ibrahimpatnam,Vijayawada-521456. He has more than Eight years of experience in teaching field. His area of interests are wireless networks & programming, & Mobile Computing.