ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

A New Unique Approach of Avoiding Forgery and Packet Drop Attacks in Wireless Sensor Networks

V.H. Sandeep Naik[1], C.H. Sudarsan Raju[2]

M.Tech Student, Department of ECE, BIT Institute of Technology, Hindupur, India[1]

Associate Professor, Department of ECE, BIT Institute of Technology, Hindupur, India[2]

ABSTRACT: The numerous applications should work in Large-scale sensor networks domains. The data collected from wireless sensor network are used in making decisions in critical infrastructures. Data's are originated from multiple sources and transmitted through intermediate processing nodes. Those nodes perform the aggregation on information. An attacker compromise those type of networks by introducing additional nodes in the network or compromising the existing nodes. So achieving the high data trustworthiness is crucial for correct decision-making. While evaluating the trustworthiness of sensor data provenance is an important factor. The several challenging requirements for provenance management in sensor networks are low energy and low bandwidth consumption, competent storage and secure transmission. This survey proposes a new lightweight scheme in order to securely transmit provenance with sensor data. The proposed in-packet Bloom filters techniques used to encode provenance with the sensor data. This mechanism initially performs provenance at the base station then perform reconstruction of the data at the base station. In addition to this the provenance scheme functionality used to detect packet drop attacks organized by malicious data forwarding nodes. This survey describes the effectiveness and efficiency of the Light weight secure provenance scheme in detecting packet forgery and packet loss attacks.

KEYWORDS: Provenance, security, sensor networks, Packet drop attack, Wireless Sensor Networks, Provenance attack.

1. INTRODUCTION

WIRELESS sensor networks are most increasingly used in several applications such as wild habitat monitoring, forest fire detection, and military surveillance area. After being deployed in the field of interest, sensor nodes organize themselves into a multihop network area with the base station. Typically, a sensor node is severely constrained in terms of computation capability and energy reserves. Sensor networks are used in numerous application domains, such as cyber physical infrastructure systems, environmental monitoring and power grids. 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. In a multi-hops sensor network and data provenance allows the BS to trace the source and forwarding path of individual data packets. 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. We propose a provenance encoding strategy whereby each node on the path of a data packet securely embeds provenance information within a Bloom filter that is transmitted along with the data. Upon receiving the packet, the Base station extracts and verifies the provenance information. We also devise an extension of the provenance encoding scheme that allows the Base station to detect if a packet drop attack was staged by a malicious node.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

II. EXISTING SYSTEM

In 2006 K. Muniswamy-Reddy et al, propose "Provenance-Aware Storage systems," .This survey states that in a multi-hop sensor network by using the data provenance scheme the BS can trace the source and forwarding path of an individual data packet. For each packet Provenance must be recorded but there is an important challenge arises due to the heavy storage, energy and bandwidth conditions of sensor nodes. So, it is necessary to provide a light-weight provenance scheme with low overhead.

Disadvantage

Sensors often operate in a untrusted environment, so there may chance of attacks. The necessary to address security requirements such as confidentiality, integrity and freshness of provenance should be increased.

In 2005 R. Hasan et al proposes "threat model for wireless sensor networks". The assumption about the BS is it should be a trusted one, but if any other arbitrary node may be attacked means the also be changed to malicious. An attacker can eavesdrop and perform traffic analysis anywhere on the path. In addition to this he/she is able to organize a few malicious nodes, as well as compromise/attack a few legitimate nodes by capturing them and physically overwriting their memory. If an attacker compromises a node means it can extract all key materials, data, and codes stored on that node. The adversary can drop, inject or alter packets on the links which are under the control of attacker. Also the attacker can create the denial of service attacks such as the complete removal of provenance. If a data packet does not contain no provenance records means it considered as highly suspicious data and hence generate an alarm/signal at the BS about this malicious packet arrival. To overcome this type of detection the attacker attempts to misrepresent the data provenance.

In 2012 S. Roy et al propose "Secure Data Aggregation in Wireless Sensor Networks," .This work deals with attacks against the synopsis diffusion. This aggregation work presents a lightweight verification algorithm to make verification at the BS. The several synopses generated should be verified independently by the verification protocol at three phases. The phases are query dissemination phase, aggregation phase and the verification phase. In the first phase called query dissemination phase, the BS broadcasts the aggregation name to compute a random seed. In second phase called the aggregation phase, each node computes a sub aggregate value based on the local value and the synopses of its children. The node also randomly selects a set of MACs .From the selected MACs check whether it should be the received ones from its children. Finally, in the third phase called verification phase, the BS computes the final synopses using the messages from its child nodes and verifies the received MACs.
In 2008 A. Ramachandran et al proposed "Packets with Provenance" .This scheme catches provenance for network packets in form of per packet tags. The captured information stores a history of all nodes and processes that packet and manipulates those packets. However, this scheme assures a trusted environment which is not practical in sensor networks.
In 2010 W. Zhou et.al proposes "Querying and Maintenance of Network Provenance at Internet- Scale" which describes the history and sub part of the network state. This result came from the execution of a distributed protocol. The disadvantage of this system is also does not address security concerns and is specific to some network use cases.

III. PROPOSED SYSTEM

The goal is to design a provenance encoding and decoding mechanism which satisfies security and performance needs. It proposes a provenance encoding strategy in that each node on the path of a data packet securely embeds provenance information within a Bloom filter (BF) should be transmitted along with the data. While receiving the packet the Base Station extracts and verifies the provenance information. The extension of the provenance encoding scheme allows the BS to detect packet drop attack organized by a malicious node. The features are:

- Formulate the problem of secure provenance transmission in sensor networks, and identify the challenges specific to this context.
- Design an effective technique for provenance decoding and verification at the base station.
- Extend the secure provenance encoding scheme and devise a mechanism that detects packet drop attacks staged by malicious forwarding sensor nodes.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

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

IMPLEMENTATION

In packet Boom Filter (iBF)

This is a distributed mechanism in order to encode provenance at the nodes and it will work as centralized algorithm to decode it at the BS. The technical core of this survey is the notion of (iBF). In this packet consists of a unique sequence number, data value, and an iBF which contains the provenance. The focus of this scheme is a securely transmitting provenance with the data to the BS. In this aggregation framework, securing the data values is an important factor,. The secure provenance technique can be used to obtain a complete solution that provides security for data, provenance and data-provenance binding.

The three Security Objectives in sensor networks is a confidentiality, Integrity and freshness.

A. SECURE PROVENANCE ENCODING

We secure provenance technique can be used in conjunction with such work to obtain a complete solution that provides Security for data provenance and data-provenance binding. We propose a distributed mechanism to encode provenance at the nodes and a centralized algorithm to decode it at the BS. The technical core of our proposal is the notion of in-packet Bloom filter (iBF). Each packet consists of a unique sequence number, data value, and an iBF which holds the provenance. We emphasize that our focus is on securely transmitting provenance to the Base station. We secure provenance technique can be used in conjunction with such work to obtain a complete solution that provides security for data provenance and data-provenance binding.

B. PROVENANCE ENCODING

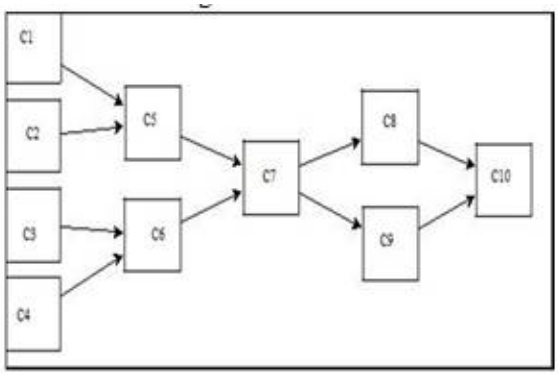

Fig1: Provenance graph

The Figure shows that to produce the final result, the contributor C5 uses the outputs of contributors C1 and C2 while contributor of C6 uses the output of contributors C3 and C4. Contributor C7 uses the output of C5 and C6 which later used by C8 and C9. C10 is the final process is executed by that processes the outputs of C8 and C9. After each process is executed and the provenance of the process we had created/generated, the provenance is stored in the provenance database. All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

C. PROVENANCE DECODING

When a Base station receives a data packet .Base station know what the data packet should be checks. Afterwards, upon receiving a packet, it is sufficient for the BS to verify its knowledge of provenance with that encoded in the packet.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

Advantages of Proposed System

The fast message authentication code (MAC) schemes and Bloom filters are fixed-size data structures that efficiently represent provenance.

- Bloom filters make efficient usage of bandwidth, and they yield low error rates
- Claim for Confidentiality: - iBF is computationally infeasible to an attacker to gain data about the sensor nodes included in the provenance.
- Claim For Integrity: - An attacker, acting as single user or colluding with others in the group cannot successfully add or legitimate nodes to the data generated by the compromised/already attack happened nodes.
- An attacker or a set of cooperative attackers cannot selectively add or remove nodes from the provenance of data generated by legitimate nodes.

IV. NETWORK SIMULATOR

The Network Simulator is the Software using and Version 2.28.Network Simulator (NS2) is a discrete event driven simulator developed at UC Berkeley. It is part of the VINT project.
The goal of NS2 is to support networking research and education. It is suitable for designing new protocols, comparing different protocols and traffic evaluations.

NS2 is developed as a collaborative environment. It is distributed freely and open source. Versions are available for FreeBSD, Linux, Solaris, Windows and Mac OS X.

NS2 is built using object oriented methods in C++and OTCL (object oriented variant of TCL).

TCL - Tool Command Language used for specifying scenarios and events.

Nam is a TCL/TK based animation tool for viewing network simulation traces and real world packet traces. It supports topology layout, packet level animation, and various data inspection tools.

V. RESULTS ANALYSIS

This section gives the simulations that were performed to evaluate of a new unique approach of avoiding forgery and packet drop attacks in wireless sensor network using the network simulator NS2 software (version 2.28).
To Analysis the performance we measure End to-End Delay and No of Transmission.

End-to-end Delay: the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

$$\mathbf{E2E=} \frac{\sum \text{Arrive time} - \text{Send time}}{\sum \text{No of connections}}$$

The Fig 2 shows the Graph End-to-end Delay Graph
The Fig 3 shows the Transmission Graph and the Fig 4 shows the NAM
The Fig 5 shows the NAM of approach of avoiding forgery and packet drop attacks in wireless sensor network using the network simulator NS2.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

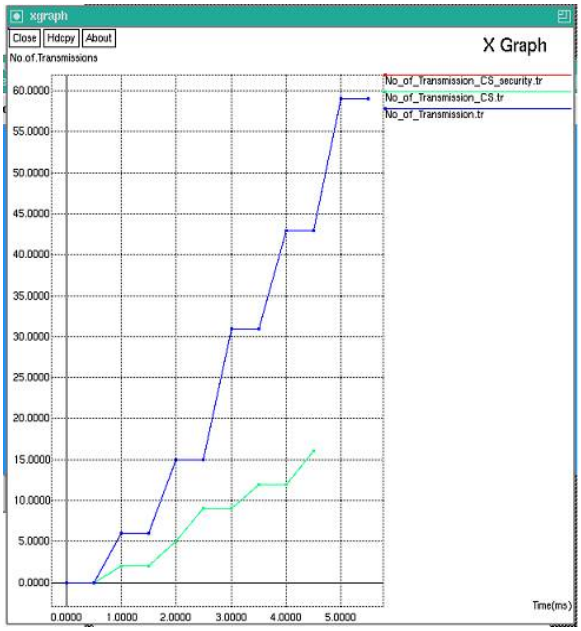

Fig 2: No of Transmission Graph.

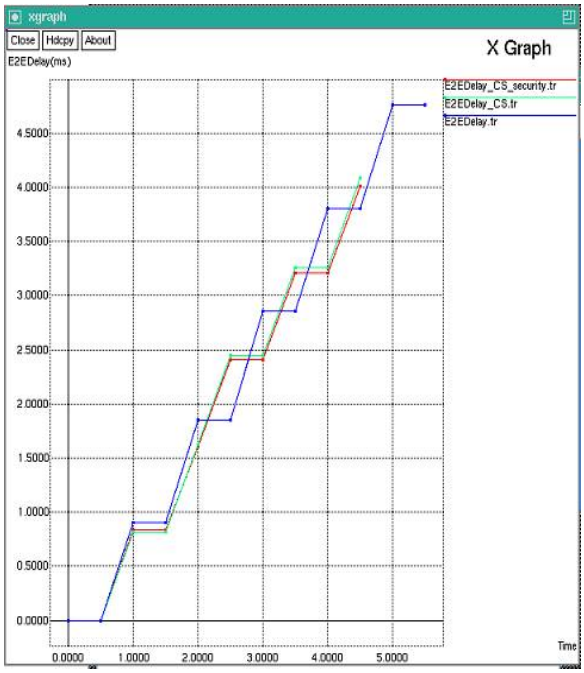

Fig 3: END- END Delay Graph

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

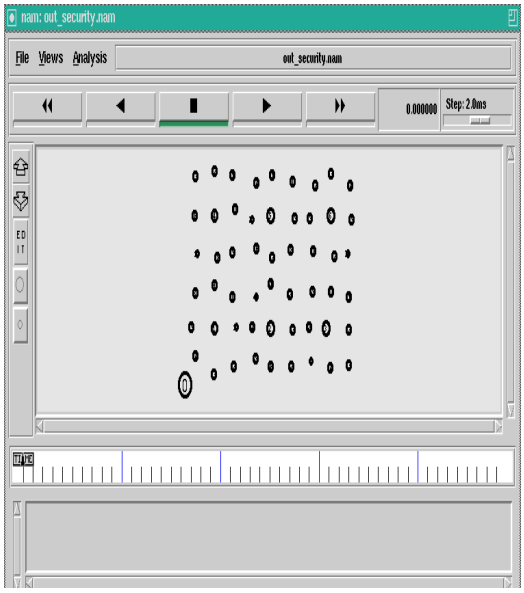

Fig 4: NAM Generation

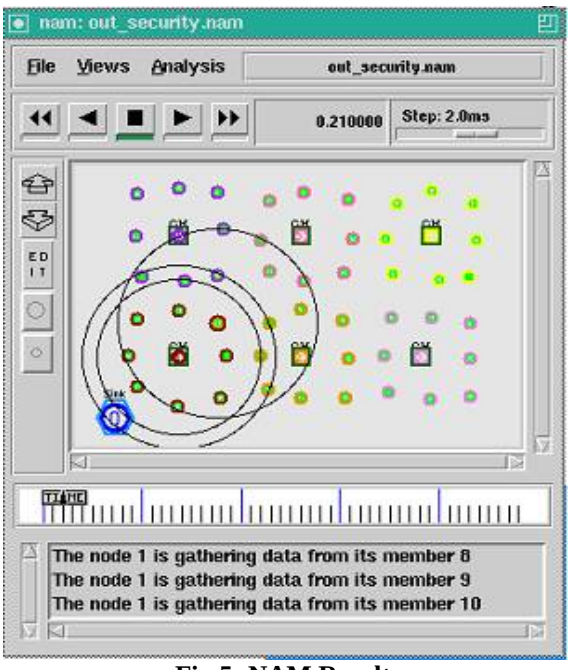

Fig 5: NAM Result

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

A. SIMULATION PARAMETERS

Parameters	Values
Simulator	NS 2.28
Protocol	AODV, DSDV
Traffic Source	TCP,UDP,IBF
Application	CYGWIN
Number of Nodes	13

Maximum Simulation Time	100 sec
Antenna	Omni Antenna
Simulation Area	1000x1000

B. PERFORMANCE RESULT ANALYSIS

Generated Packet	680
Received Packet	430
Packet Delivery Ratio	71.47%
Total Dropped Packets	250
End to End Delay	35.288ms

VI. CONCLUSION AND FUTURE SCOPE

This survey addressed the problem of how securely transmitting provenance for sensor networks. Based on Bloom filters this paper proposed a light-weight provenance encoding and decoding scheme. The scheme ensures confidentiality, integrity and freshness of provenance. Also this scheme extended to incorporate data-provenance joining, and to include packet sequence information that supports detection of packet loss attacks. The proposed scheme is considered as effective, light-weight and scalable. This survey plan implements a real system prototype of secure provenance scheme, and to increase the accuracy of packet loss detection, especially in the case of multiple uninterrupted malicious sensor nodes.

REFERENCES

[1]I. Foster, J. Vockler, M. Wilde, and Y. Zhao, “Chimera: A Virtual Data System for Representing, Querying, and Automating Data Derivation,” Proc. Conf. Scientific and Statistical Database Management, pp. 37-46, 2002.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

[2]K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, "Provenance-Aware Storage systems," Proc. USENIX Ann. Technical Conf., pp. 4-4, 2006.
[3]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.
[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]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.
[6]Y. Simmhan, B. Plale, and D. Gannon, "A Survey of Data Provenance in E-Science," ACMSIGMODRecord, vol. 34, pp. 31-36, 2005.
[7]A. Ramachandran, K. Bhandankar, M. Tariq, and N. Feamster, "Packets with Provenance," Technical Report GT-CS-08-02, Georgia Tech, 2008.
[8]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.
[9]W. Zhou, Q. Fei, A. Narayan, A. Haeberlen, B. Loo, and M. Sherr, "Secure Network Provenance," Proc. ACMSOSP, pp. 295-310, 2011.
[10]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.

BIOGRAPHY

Mr. V H SANDEEPNAIK received Bachelor's Degree in Electronics and communication Engineering from BIT Institute of Technology, Hindupur affiliated to JNTU, Anantapur. Andhra Pradesh and Studying Master's degree in Digital Systems and Computer Electronics in BIT Institute of Technology, Hindupur affiliated to JNTU, Anantapur, Andhra Pradesh.

Mr. C.H.Sudarsan Raju received Bachelor's Degree in Electrical and Electronics Engineering from SJMIT, Chitradurga, Karnataka and Master's degree in Digital Systems and Computer Electronics from JNTU, Anantapur. He is a life time member of Indian Society for Technical Education (ISTE).He is also a life time member of IMAPS. He is currently working as Associate Professor with Department of Electronics and Communication Engineering in BIT Institute of Technology, Hindupur. His research interests include wireless networks and Vehicular Ad Hoc and Sensor Networks.