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)

Website: www.ijareeie.com

Vol. 6, Issue 2, February 2017

Accurate Detection of Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks

K.Murthy Raju[1], B.Srinidhi[2]

Assoc. Professor, Department of ECE, Shri Vishnu Engineering College for women, Andhra Pradesh, India[1]

Asst. Professor, Department of ECE, Shri Vishnu Engineering College for women, Andhra Pradesh, India [2]

ABSTRACT: Wireless sensor networks are most increasingly used in several applications such as wild habitat monitoring, forest fire detection and military surveillance area. Large-scale sensor networks are deployed in numerous application domains, and the data they collect are used in decision-making for critical infrastructures. Data are streamed from multiple sources through intermediate processing nodes that aggregate information. 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 represents a key factor in evaluating the trustworthiness of sensor data. Provenance management for sensor networks introduces several challenging requirements, such as low energy and bandwidth consumption, efficient storage and secure transmission. Therefore, we propose a novel light weight scheme to securely transmit provenance for sensor data. The proposed technique relies on in-packet Bloom filters to encode provenance. We introduce efficient mechanisms for provenance verification and reconstruction at the base station. In addition, we extend the secure provenance scheme with functionality to detect packet drop attacks staged by malicious data forwarding nodes. We evaluate the proposed technique both analytically and empirically, and the results prove the effectiveness and efficiency of the light weight secure provenance scheme in detecting packet forgery and loss attacks.

KEYWORDS: Sensor Networks, Light weight secure Provenance, Detecting Packet forgery, Bloom Filter, Packet Dropping Attack, Packet Drop due to Attacker or Congestion

I. 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 data that drives such systems is produced by a variety of sources, ranging from other systems down to individual sensors and processed by multiple intermediate agents. This diversity of data sources accelerates the importance of data provenance to ensure secure and predictable operation of the streaming applications.

Data provenance is considered as an effective tool for evaluating data trustworthiness, since it summarizes the history of the ownership and the actions performed on the data. Recent research works on the provenance-based evaluation of the trustworthiness of sensor data, location data, and multi-hop network manifest the key contribution of provenance in data streams. As an example consider a battlefield surveillance system that gathers enemy locations from various sensors deployed in vehicles, air-crafts, satellites, etc. and manages queries over these data. Mission critical applications in such a system must access only high confidence data in order to guarantee accurate decisions. Thus, the assurance of data trustworthiness is crucial here, which prioritizes the secure management of provenance. Likewise, provenance plays a key role in process control tasks that analyze the real time data collected from different sensors. Provenance facilitates such systems by leveraging high trustworthy data, thus, preventing wrong control decisions. The

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)

Website: www.ijareeie.com

Vol. 6, Issue 2, February 2017

significance of provenance for streaming data is also emphasized in the Research and Development Challenges for National Cyber Security report which recommends research initiatives on efficient and secure implementation of provenance for real-time systems.

II. LITERATURE SURVEY

A Source Path Isolation Engine (SPIE) to enable IP trace back, the ability to identify the source of a particular IP packet given a copy of the packet to be traced, its destination, and an approximate time of receipt. Historically, tracing individual packets has required prohibitive amounts of memory; one of SPIE's key innovations is to reduce the memory requirement down to 0.5% of link bandwidth per unit time through the use of Bloom filters. By storing only packet digests, and not the packets themselves, SPIE also does not increase a networks vulnerability to eavesdropping. SPIE therefore allows routers to efficiently determine if they forwarded a particular packet within a specified time interval while maintaining the privacy of unrelated traffic. The advantages of this approach are SPIE implements an auditing technique while reducing storage requirements significantly, Auditing is accomplished by computing and storing a packet digest and Privacy is maintained. The major disadvantage of this approach is its deployment at high speed networks has still been a challenging task due to the high storage overhead and access time requirement for recording packet digest.

As increasing amounts of valuable information are produced and persist digitally, the ability to determine the origin of data becomes important. In science, medicine, commerce, and government, data provenance tracking is essential for rights protection, regulatory compliance, management of intelligence and medical data, and authentication of information as it flows through workplace tasks. The Case of the Fake Picasso system is to provide strong integrity and confidentiality assurances for data provenance information. It describes the provenance-aware system prototype that implements provenance tracking of data writes at the application layer, which makes it extremely easy to deploy. The advantages of this approach are it provides fine grained control over the visibility of provenance information and ensures that no one can add or remove entries in the middle of a provenance chain without detection and It reduces the overhead. The disadvantages of this approach are this may cause privacy issues, no nodes can really hide their identity since they must put their public key in the records and also, it is normal that some nodes' keys get revoked/refreshed or some nodes leave the network, it will become hard to verify their previous sent provenance records especially for a long-history provenance.

The design space of In-packet Bloom filters in depth and evaluated new ways to enrich iBF-based networking applications without sacrificing the Bloom filter simplicity. First, the power of choices extension shows to be a very powerful and handy technique to deal with the probabilistic nature of hash-based data structures, providing finer control over false positives and enabling compliance to system policies and design optimization goals. Second, the space-efficient element deletion technique provides an important probabilistic capability without the overhead of existing solutions like counting Bloom filters and avoiding the limitations of false negative-prone BF extensions. Third, security extensions were considered to couple iBFs to time and packet contents, providing a method to secure iBFs against tampering and replay attacks. Finally, have a validated the extensions in a rich simulation set-up, including useful recommendations for efficient hashing implementations. The advantages of this approach are To increase the system performance, to enable false-negative-free element deletion and to provide security-enhanced constructs at wire speed. The advantages of this approach are It is not extendable to internet-size topologies and it is very sensitive to the distribution of flows per action; i.e., to the sizes of the area.

Secure In-network processing of Exact SUM queries as well as their derivatives, e.g., COUNT, AVG, etc. satisfying all four security properties. SIES achieves this goal through a combination of homomorphic encryption and secret sharing. It is scalable as it does not involve the participation of the sensors in the verification process. It entails a small constant communication cost per network edge. Moreover, it requires few and inexpensive cryptographic operations hashes and modular additions/multiplications at each party involved. The above render SIES lightweight and, thus, an ideal solution for resource-constrained sensors. The advantages of this approach are it is satisfying all the necessary security properties of the targeted model, data confidentiality, integrity, authentication, and freshness and it achieves this goal through a combination of a homomorphic encryption scheme and a secret sharing method. The major disadvantage of

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)

Website: www.ijareeie.com

Vol. 6, Issue 2, February 2017

this approach is some provides perfect authentication but they either impose extra overhead for computation or provides delayed authentication. Many provide integrity protection with some assumptions with privacy homomorphism.

TinySec addresses security in devices where energy and computation power present significant resource limitations. It has designed TinySec to address these deficiencies using the lessons we have learned from other security protocols. It has tried to highlight design process from a cryptographic perspective that meets both the intended resource constraints and security requirements. TinySec relies on cryptographic primitives that have been vetted in the security community for many years. TinySec implementation is in wide use throughout the sensor network community. We know of researchers building key exchange protocols on top of TinySec. Others have ported TinySec to their own custom hardware. TinySec is simple enough to integrate into existing applications that the burden on application programmers is minimal. The advantages of this approach are it is configurable and flexible security features that can be tailored to the needs of the application under consideration and it can be used as a ready-to-use experimental test-bed for security related experimentations in WSN. The major disadvantages of this approach is using a hardware based solution lacks flexibility and does not provide the transparent security enablement in the WSN applications.

III. SYSTEM ANALYSIS

In the existing system, the key contribution of provenance in systems Where the use of untrust worthy data may lead to catastrophic failures SCADA systems. Although provenance modeling, collection, and querying have been studied extensively for workflows and curated databases, it is cannot detect the packet dropping attack launched through provenance forgery. Provenance in the sensor networks has not been properly addressed. The disadvantages of existing system are Traditional provenance security solutions use intensively cryptography and digital structures, and they employ append-based data structures to store provenance leading to high costs and also, It employs separate transmission channels for data and provenance.

The problem of secure and efficient provenance transmission is addressed and provenance verification is applied to detect packet loss attacks staged by malicious sensor nodes. In a multi-hop sensor network, data provenance allows the base station 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 constraints of sensor nodes. The main goal is to design a provenance encoding and decoding mechanism that satisfies such security and performance needs. A provenance encoding strategy is proposed 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 base station extracts and verifies the provenance information. It also devises an extension of the provenance encoding scheme that allows the BS to detect if a packet drop attack was staged by a malicious node. It uses 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.

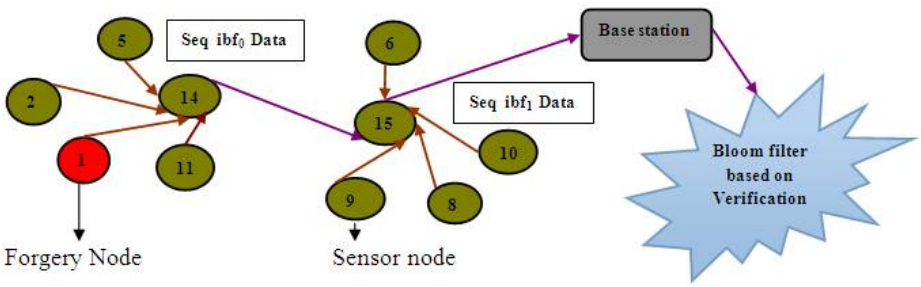

Fig. 1 Architecture of provenance forgery

Packet dropping in the network may due to several reasons in the network. Proposed scheme does not classify the packet dropping that arises due to congestion in the path which leads to false negative. Hence a technique PDAC is

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)

Website: www.ijareeie.com

Vol. 6, Issue 2, February 2017

contributed that classifies packet dropping due to congestion or attacker and detects attacker accurately. BS collects the routing load on every router in the path and classifies packet loss reason. Routing load refers to the number of data flows the node involved. If it involves in more number of flows then probability packet dropping at the node is high. This technique classifies dropping reason accurately and improves attack detection accuracy.

There are 6 steps in implementing the complete procedure. They are

- Secure Provenance Encoding using Bloom Filter
- Provenance Verification and Provenance Collection
- Provenance Encoding for detecting Packet Dropping Attack
- Verification and Collection of Packet Dropping Attack
- PDAC: Accurate Detection of Packet Dropping Attack using routing load
- Performance Evaluation

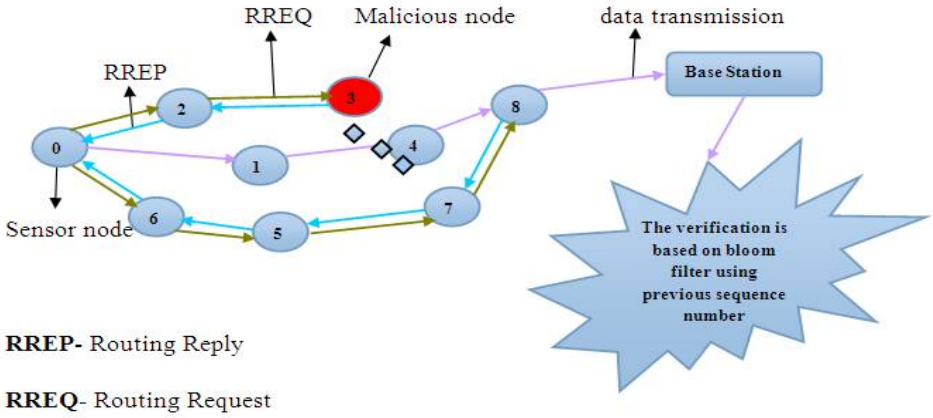

Fig. 2 Architecture of packet dropping attack

The advantages of this proposed system are Low energy and bandwidth consumption, efficient storage and secure transmission. It proves the effectiveness and efficiency of the light weight secure provenance scheme in detecting packet forgery and loss attack. It extends the secure provenance encoding scheme and devise a mechanism that detects packet drop attacks staged by malicious forwarding sensor nodes.

Bloom filters (BF) have increasingly become a fundamental data aggregation component to address performance and scalability issues of very diverse network applications, including overlay networks, data-centric routing, traffic monitoring, and so on. In this work, focus on the subset of distributed networking applications based on packet-header-size Bloom filters to share some state information set among network nodes. The specific state carried in the Bloom filter varies from application to application, ranging from secure credentials to IP prefixes and link identifiers, with the shared requirement of a fixed-size packet header data structure to efficiently verify set memberships. Considering the constraints faced by the implementation of next generation networks e.g. Gbps speeds, increasingly complex tasks, larger systems, high-speed memory availability, etc., recent inter-networking chose to include more information in the packet headers to keep pace with the increasing speed and needs of Internet-scale systems. Moving state to the packets themselves helps to alleviate system bottle necks and enables new in-network applications or stateless protocol designs. The BF used in this type of applications as an in-packet Bloom filter (iBF). These specific needs may benefit from additional capabilities like element removals or security enhancements.

IV. RESULT AND DISCUSSION

Most of these studies and works have been based on the use of simulators. Network simulator ns-2 has been the most used network simulator for these studies. NS2 is an open-source event-driven simulator designed specifically for research in computer communication networks. NS2 now contains modules for numerous network components such as

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)

Website: www.ijareeie.com

Vol. 6, Issue 2, February 2017

routing, transport layer protocol, application, etc. To investigate network performance, researchers can simply use an easy-to-use scripting language to configure a network, and observe results. Network simulator ns-2 can be defined as a simulator that is written in two languages, C++ and OTcl (object-oriented tool command language), with the concept of object oriented. The topology of simulation is written with Tcl, and it has been linked with the modules of the simulator that are written in C++ through the use of OTcl linkages.

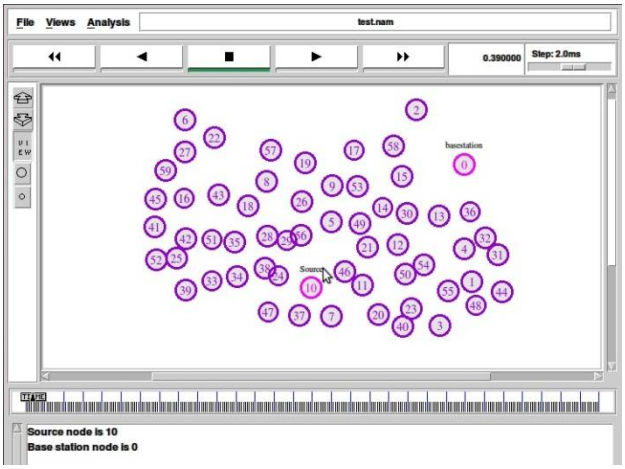

Fig. 3 Generation of nodes in network animator window

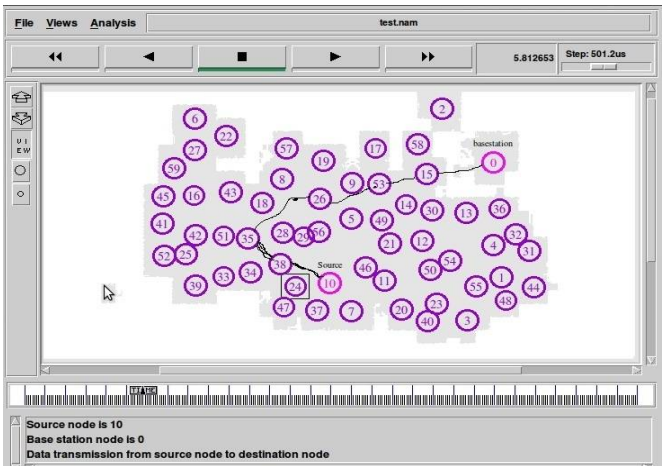

Fig. 4 Data transmission from source to destination

In figure 5 Data transmission route before attacker is launched 1-77-30-60-36-46-69-28-0. Similarly in figure 6 Data transmission route 64-91-50-63-61-2-4-0 when attacker is launched.

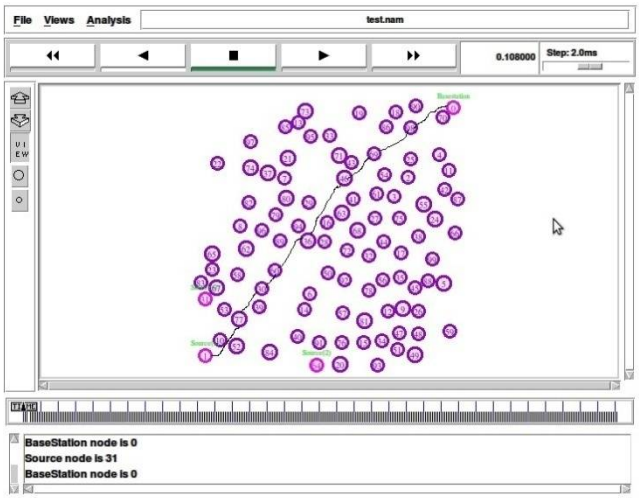

Fig. 5 Data transmission before attacker is launched

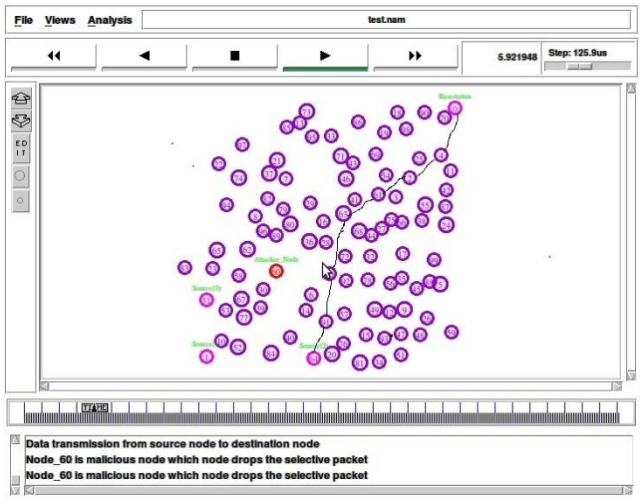

Fig. 6 Data transmission after attacker is launched

If the difference value between current sequence number and previous sequence number less than 5 it's not an attacker node. Otherwise is an attacker node. In the suspicious list of node involved attacker node and genuine node. So these nodes divide separately. We will calculate the generated packet count and received packet count of source side and receiver side. This suspicious list of all nodes checks the generated packet count and received packet count. Then, finds the difference between generated packet count and received packet count. If the difference is less than 25 it is not an attacker node. Otherwise it is an attacker node. Proposed and enhanced protocols are compared for the scenarios of varying number of hops. Communication range is varied as 200m, 250m, 300m and 350m to vary the hops as 4, 3.2, 2.6 and 2.3 hops respectively. Scenario is kept same for both protocols with same topology, energy, number of flows

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)

Website: www.ijareeie.com

Vol. 6, Issue 2, February 2017

and number of nodes. Totally 4 simulation runs are made by varying number of hops as 4, 3.2, 2.6, and 2.3. Parameters such as energy consumption, packet loss rate or dropped packet, packet delivery ratio and detection accuracy are computed and plotted as Xgraph.

With variation of number of hops the detection accuracy is better in Packet drop due to congestion or attacker scheme when compared to existing packet dropping attacker scheme shown in figure 7, dropped packets or packet loss rate is similar in both Packet dropping attack scheme and packet drop due to congestion or attacker scheme shown in figure 8

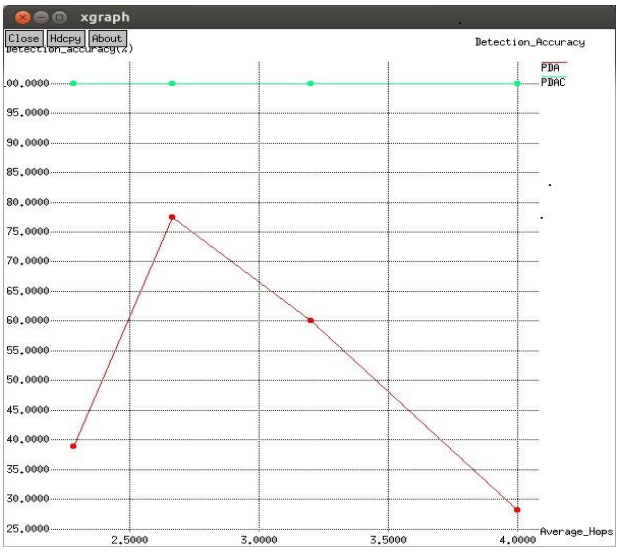

Fig. 7 Comparison of detection accuracy between PDA and PDAC

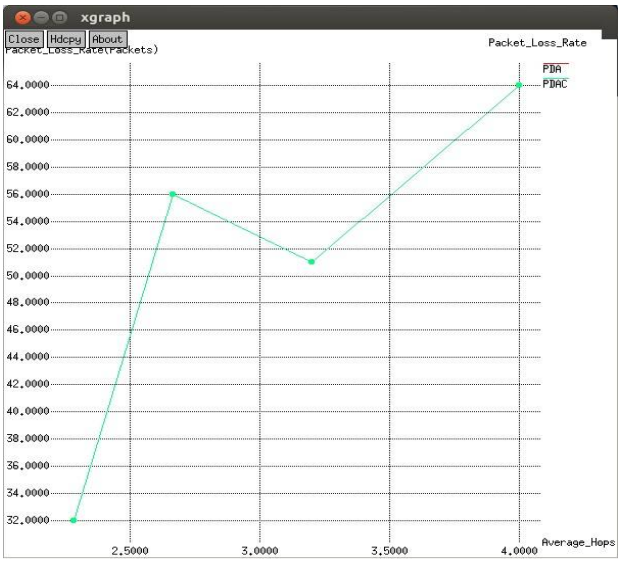

Fig. 8 Comparison of Packet loss rate between PDA and PDAC

With variation of number of hops the energy consumption is shown in figure 9 and the packet delivery ratio is shown in figure 10 similar in both Packet dropping attack scheme and packet drop due to congestion or attacker scheme.

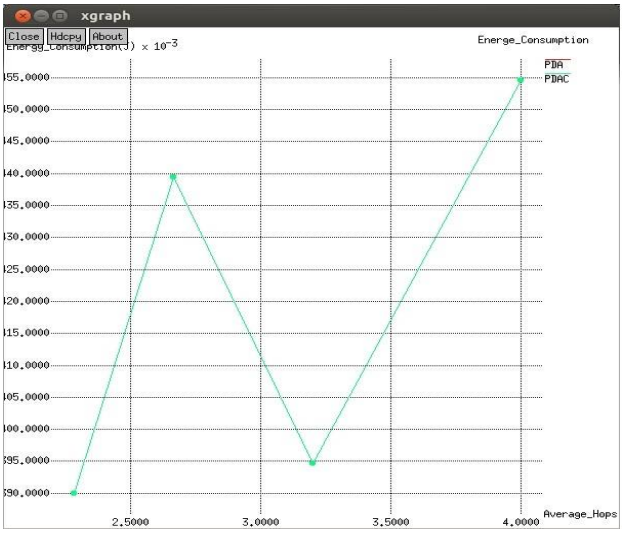

Fig. 10 Comparison of Packet delivery ratio between PDA and PDAC

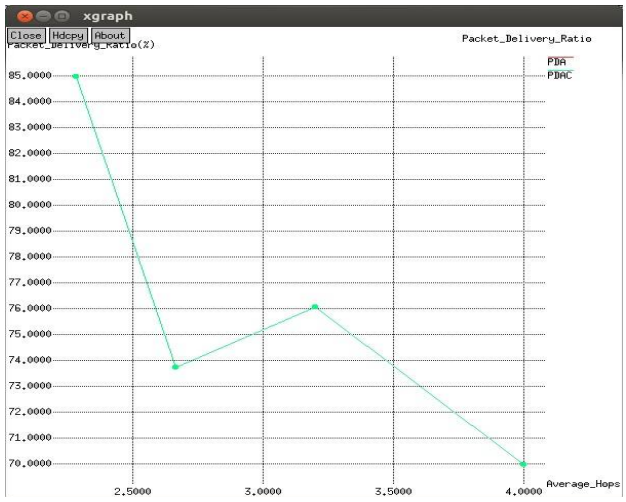

Fig. 9 Comparison of energy consumption between PDA and PDAC

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)

Website: www.ijareeie.com

Vol. 6, Issue 2, February 2017

V. CONCLUSION

The problem of securely transmitting provenance for sensor networks has been solved by proposing 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. Packet dropping attack detection accuracy is improved through the PDAC technique that classifies the node as genuine or attacker based on packet dropping reason either due to congestion or intentional drop by attacker respectively. Experimental and analytical evaluation results show that the proposed scheme is effective, light-weight and scalable.

REFERENCES

[1] Alex C. Snoeren, Craig Partridge, Fellow, Luis A. Sanchez, Christine E. Jones, Fabrice Tchakountio, Beverly Schwartz, Stephen T. Kent, and W. Timothy Strayer, "Single-Packet IP Traceback" IEEE/ACM Transactions on Networking, Vol. 10, No. 6, pp. 721-734, 2002.

[2] Ragib Hasan, Radu Sion and Marianne Winslett, "The Case of the Fake Picasso: Preventing History Forgery with Secure Provenance"In FAST, Vol. 9, pp. 1-14, 2009.

[3] Christian Esteve Rothenberg, Carlos A. B. Macapuna, Maurcio F. Magalh esa, F bio L. Verdib , Alexander and Wiesmaierc, "In-packet Bloom filters: Design and networking applications" Computer Networks, Vol. 55, No. 6, pp. 1364-1378, 2011.

[4] Minos Garofalakis, Joseph M. Hellerstein and Petros Maniatis, "Proof Sketches: Verifiable Multi-Party Aggregation" Technical Report EECS Department, 2006.ss

[5] Stavros Papadopoulos, Aggelos Kiayias and Dimitris Papadias, "Secure and Efficient In-Network Processing of Exact SUM Queries" In Data Engineering (ICDE), 27th International Conference on, IEEE, pp. 517-528, 2011.

[6] Wenchao Zhou, Micah Sherr, Tao Tao, Xiaozhou Li, Boon Thau Loo and Yun Mao, "Efficient Querying and Maintenance of Network Provenance at Internet-Scale" In Proceedings of the SIGMOD International Conference on Management of Data, ACM, pp. 615-626, 2010.

[7] Chris Karlof, Naveen Sastry and David Wagner, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks" In Proceeding of Second International Conference on Embedded Networked Sensor Systems, ACM, pp. 162-175, 2004.