Middle-East Journal of Scientific Research 24 (Techniques and Algorithms in Emerging Technologies): 182-187, 2016
ISSN 1990-9233;

DOI: 10.5829/idosi.mejsr.2016.24.TAET23425

Provide Secure Transmission to Avoid Packet Drop Attacks in WSNs

[1]B. Poovizhi and [2]M.M. Kokila

[1]Department of Computer Science and Engineering (with Specialization in Networks,
Vivekanandha Institute of Engineering and Technology for Women, Tiruchengode, India
[2]Department of Computer science and Engineering,
Vivekanandha Institute of Engineering and Technology for Women, Tiruchengode, India

Abstract: Large-scale sensor networks are deployed in various application areas and the records they collect are used in decision-making for vital infrastructures. Data are streamed from multiple sources through intermediate processing nodes that aggregate information. A malicious opponent may introduce additional nodes in the network or compromise existing ones. Therefore, assuring high data trustworthiness is critical for correct decision-making. Data provenance represents a key feature in evaluating the honesty of sensor data. Provenance management for sensor networks introduces several challenging requirements, such as low bandwidth and energy consumption, efficient storage and secure transmission. A new lightweight scheme to securely transmit provenance for sensor data. The proposed technique relies on in-packet Bloom filters to encode the provenance. The competent mechanisms for provenance verification and reconstruction at the base station. The secure provenance scheme with functionality to detect packet drop attacks staged by malicious data forwarding nodes. The proposed technique was evaluated both analytically and empirically and the results verify the efficiency and effectiveness of the lightweight secure provenance scheme in detecting packet forgery and loss attacks.

Key words: Provenance · Security · Sensor networks

INTRODUCTION

Network security has become more important for personal computer users, organizations and the military. With the introduction of the internet, security became a major issue and the history of the security permits a better understanding of the appearance of security technology. The internet design itself allowed for many security threats to occur. The design of the internet, when personalized can reduce the possible attacks that can be sent across the network [1]. Knowing the attack methods allows for the proper security to come forward. Many business secure themselves from the internet through firewalls and encryption mechanisms. The businesses create an "intranet" to stay connected to the internet but protected from possible threats.

Network security is becoming of great importance because of rational property that can be easily acquired through the internet. Two fundamentally different networks named as data networks and synchronous network comprised of switches.

The internet is considered a data network. Since the modern data network consists of computer-based routers, information can be taken by special programs, such as "Trojan horses," placed in the routers. The synchronous network that consists of switches does not buffer data and therefore are not threatened by attackers. That is why security is highlighted in data networks, such as the internet and other networks that link to the internet.

When developing a secure network, the following need to be considered:

- Access – authorized users are afforded the means to communicate to and from a exact network
- Confidentiality – Information in the network ruins private
- Authentication – Ensure the true users of the network
- Integrity – Ensure the message has not been modified in its transmission.
- Non-repudiation – Ensure the user does not decline that he used the network

Corresponding Author: B. Poovizhi, Department of Computer Science and Engineering (with Specialization in Networks, Vivekanandha Institute of Engineering and Technology for Women, Tiruchengode, India.

Wireless Sensor Networks: A Wireless Sensor Network is a self-arranging network of small sensor nodes communicating between themselves using radio signals and positioned in quantity to sense, monitor and understand the physical world. Wireless Sensor nodes are called 'motes'. Bridge is provided between the real physical and virtual [2] worlds by WSN which allows the ability to detect the previously unobservable at a fine resolution over large spatiotemporal scales. Have a wide range of potential applications to industry, civil infrastructure, transportation, science and security.

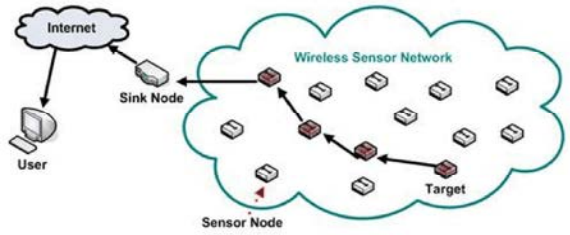

Fig. 1: Wireless sensor network

The cost of sensor nodes is parallelly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. In sensor nodes, the size and cost limits result in corresponding constraints on resources such as memory, energy, communications bandwidth and computational speed. The topology of the WSNs can differ from a simple star network to an advanced multi-hop wireless mesh network.

Applications

- Seismic Monitoring
- Automated Building Climate Control
- Industrial Process Monitoring
- Monitoring Groundwater Contamination
- Rapid Emergency Response
- Civil Structural Health Monitoring
- Perimeter Security and Surveillance
- Habitat and Ecosystem Monitoring

Characteristics: The main characteristics of a WSN include:

- Mobility of nodes
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Reliability
- Ability to with stand harsh environmental conditions
- Power consumption is checked for nodes using batteries or energy harvesting
- Ease of use
- Performance can be measured
- Availability
- Ability to cope with node failures (resilience

Security In Sensor Networks: Wireless sensor networks (WSN) [3] are generally set up for collecting records from insecure environment. Nearly all security protocols for WSN believe that the adversary can achieve entirely control over a sensor node by way of direct physical access. Security goals in sensor networks depend on the need to know what we are going to protect. We conclude four security goals in sensor networks which are Confidentiality, Integrity, Authentication and Availability (CIAA).

- Confidentiality is the ability to obscure message from a passive attacker, where the message communicated on sensor networks stays confidential.
- Integrity refers to the ability to confirm the message has not been messed, altered or changed on the network.
- Authentication Need to know if the messages are from the node it maintains to be from, determining the reliability of message's origin.
- Availability is to establish if a node has the ability to use the resources and the network is available for the messages to move on.

Attacks in Wireless Sensor Networks:

- Denial Of Services (Dos)
- Attacks On Time Synchronization Protocols
- Software Attacks
- Routing Attacks
- Traffic Analysis Attacks
- Sybil Attacks
- Attacks On In-Network Processing
- Replication Attacks
- Node Capture Attack

Data Provenance in Sensor Networks: Sensor networks are used in application domains, examples are cyber physical infrastructure, environmental monitoring, 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 judge data trustworthiness [4] and the actions performed on the data. We inspect the difficulty of efficient provenance

transmission and secure and handling for sensor networks and we use provenance to detect packet loss attacks staged by malicious sensor nodes. In a multi-hop sensor network the data provenance [5] is to allow the Base Station to trace the source and forwarding path of a specific data packet the provenance must be record for each an every packet, but important challenges arise due to some reason the first is tight storage [6], energy and bandwidth limitations of sensor nodes. Therefore it is necessary devise a light-weight provenance solution with low overhead. Sensors should operate in untrusted environment, where they may be happens subject to attacks. That's why it is necessary to address security requirements such as privacy, reliability and cleanness of provenance. Our project goal is to design a provenance encoding and decoding tool that would be satisfies such safety and presentation needs.

We Design propose a provenance encoding strategy where each node on the track of a data packet securely embeds provenance information within a Bloom filter that is conveyed along with the data. Receiving the packet the Base Station should be extracts and verifies the provenance information. The provenance encoding system that allows the Base Station to detect if a packet drop attack was staged by a malicious node.

We use fast Message Authentication Code [7] and Bloom filters (BF), which are stable size data structures that efficiently represent provenance wireless networks of sensor devices Sensor networks of the future are intended to consist of hundreds of cheap nodes, that can be readily deployed in physical situations to collect useful information.

Our motivation on the subsection of distributed networking applications created on packet header-size Bloom filters to share some state between network nodes. The specific state carried in the Bloom filter differs 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 well verify set memberships. Bloom filters make effective usage of bandwidth and they yield low error rates in practice. Our specific contributions are:

The problem of secure provenance [8] transmission is formulated in sensor networks.

- The implementation of an in-packet Bloom filter provenance encoding Scheme.
- To design efficient techniques for provenance decoding and verification at the base station.
- To design mechanism that detects packet drop attacks staged by malicious forwarding sensor nodes.

Packet Drop Attacks: The Simplicity in Wireless Sensor Network with resource constrained nodes makes them extremely vulnerable to variety of attacks. In a Wireless sensor networks sensor nodes check the environment, detect events of interest, produce data and collaborate in forwarding the data towards to a sink, which could be a gateway, base station or storage node. Securing the Wireless Sensor Networks need to make the network maintain all security properties: confidentiality, integrity, authenticity and availability [9].

A sensor network is often positioned in an unattended and aggressive environment to perform the monitoring and data collection tasks. When it is arranged in such an environment, it needs physical protection and is focus to node compromise. After compromising one or multiple sensor nodes, an challenger may initiate various attacks to disrupt the in-network communication. Among these attacks, two are very common dropping packets and modifying packets, i.e., compromised nodes drop or modify the packets that they are considered to forward.

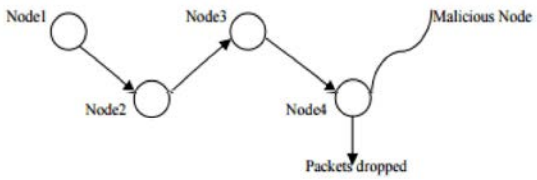

Fig. 2: Packet drop attack

Packet dropping [10]is a bad node that drops all or some of the packets that are thought to be forwarded. It may also drop the data generated by itself for some malicious reason such as blaming innocent nodes. This paper recommends a scheme to catch both packet droppers and modifiers. At first routing tree is founded using DAG. Data is transmitted beside the tree structure toward the sink. A packet sender or promoter adds a small number of extra bits, which is called packet marks, is designed such that the sink can obtain the dropping ratio correlated with every sensor node. Node categorization algorithm to identify nodes that are droppers / modifiers for sure or are guarded droppers/ modifiers.

Secure Transmission Process: A novel lightweight scheme is proposed to transmit provenance in a secure way for sensor data. Furthermore, as an enhancement the secure provenance scheme with functionality to detect packet drop attacks staged by malicious data forwarding nodes. The ip address of the node to which the data packet is transmitted is used as the secret key. This technique works on in-packet Bloom filters [11] to encode provenance.

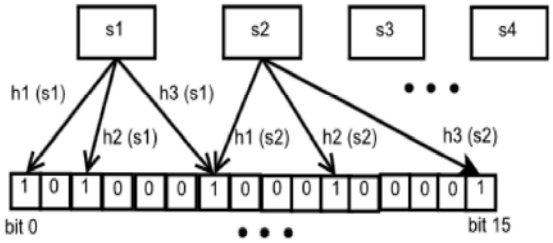

Fig. 3: Bloom Filter

The BF is a space-efficient data structure for probabilistic demonstration of a set of items. Some applications that use Bloom filters [12]need to communicate these filters across the network. In this case, besides the three performance metrics we have seen so far:

- The computational transparency to lookup a value (related to the number of hash functions used),
- The size of the filter in memory and
- The error rate, a fourth metric can be used: the size of the filter transmitted across the network.

The bloom filter uses the ip address as a key and encode the data packet for transmission. Hence the attacker cannot decrypt the data without knowing the key value. The proposed technique was evaluated 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.

System Architecture: The data packet is transmitted from the sender to the receiver. The node has encrypted with the key. At receiving site the file has asked for the key to decrypt the packet. If the packet receives at the correct site with the key value, the content displayed. Otherwise an encrypted format is displayed. And an packet drop attack acknowledgement is send to the sender.

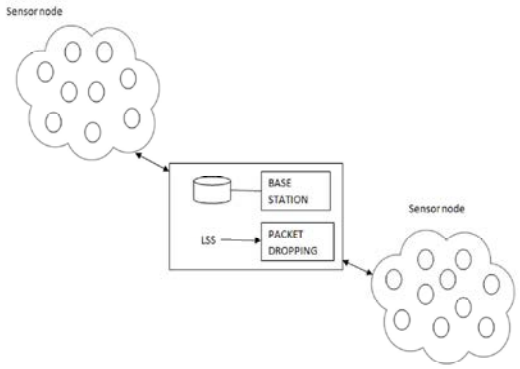

Fig. 4: System Architechture

Network Model: Consider a multihop wireless sensor network, consisting of a number of sensor nodes and a base station that collects data from the network. Sensor nodes are motionless after deployment, but routing paths may change over time, e.g., due to node failure. Each node reports its near by (i.e., one hop) node information to the BS after deployment. Assume a multiple-round process of data collection Each sensor generates data periodically and individual values are collected towards the BS using any existing hierarchical (i.e., tree-based) dissemination scheme Sensor nodes are stationary after deployment, but routing paths may change over time, e.g., due to node failure.

Provenance Encoding: For a data packet, provenance encoding refers to generating the vertices in the provenance graph and inserting them into the iBF. Each vertex originates 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. A block cipher function is used to produce this VID in a secure manner.

Provenance Forgery and Packet Drop Attacks: The secure provenance encoding scheme is extended to detect packet drop attacks and to identify malicious node (s). Assume the links on the path exhibit natural packet loss and several adversarial nodes may exist on the path. For simplicity, consider only linear data flow paths.

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 belonging to 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 be a mismatch between the acknowledgements generated from different nodes on the path.

Provenance Decoding: Not only the intermediate nodes, but also the BS stores and updates the latest packet sequence number for each data flow. Upon receiving a packet, the BS retrieves the preceding packet sequence transmitted by the source node from the packet header, fetches the last packet sequence for the flow from its local storage and utilizes these two sequences in the process of provenance verification and collection. Provenance BS first executes the provenance verification process upon receiving a packet.

The BS knows the current data path for the packet (decoded from the provenance of the previous packet in the flow) and the preceding packet sequence number forwarded by each node in the path. In this context, the BS assumes that each node in the path saw and forwarded the same packet in the last round and that this packet's sequence number is the same one as recorded at the BS.

Verification failure here indicates either a change in the data flow path, a packet drop attack or a BF modification attack and triggers the provenance collection process. Collection attempts to retrieve the nodes from the encoded provenance, confirm a packet loss and identify the malicious node that dropped the packet. It also distinguishes between the packet drop attack and other attacks that might have altered the iBF.

Secure Packet Dropping: We introduce an addition key which one is used in existing system encryption key that is the reviser IP which means except reviver no one can decrypt the file content. And another key lock key random OTP has to been sended to mobile via SMS. This OTP is used to unlock the file.

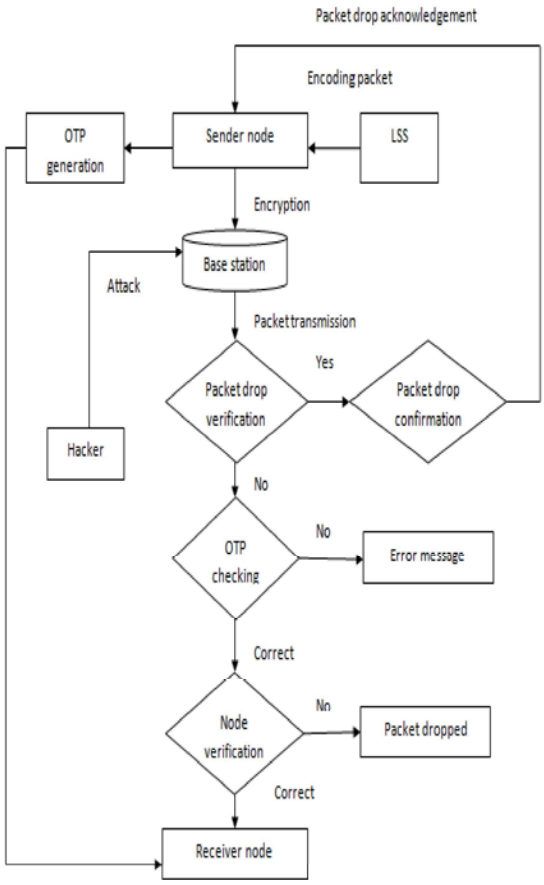

Fig. 5: Data flow diagram

CONCLUSION

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, freshness and integrity of provenance. We extended the scheme to incorporate data-provenance binding and to addpacket 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 proposed system, A log key of this secure provenance scheme to be used to improve the accuracy of packet loss detection, especially in the case of multiple consecutive malicious sensor nodes.

ACKNOWLEDGMENT

This research was supported by my Head of the Department, Prof.T.R.Srinivasan. We thank Mr.Chandra Mohan for assistance with a technique and Mr.Sathish for comments that greatly improved the manuscript. We thank famous persons Dr.Karunanithi and Dr.K.C.K.Vijayakumar, for sharing their pearls of wisdom with us during the course of this research and we thank Mr.J.Jeyaram and Mr.R.Rajagopal reviewers for their so-called insights. We also immensely grateful to family for their comments and support, although any errors are our own and should not taint the reputations of these esteemed persons.

REFERENCES

1. Dasgupta, K., K. Kalpakis and P. Namjoshi, 2003. An Efficient Clustering Based Heuristic for Data Gathering and Aggregation in Sensor Networks, Proc. Wireless Comm. and Networking Conf., pp: 1948-1953.
2. Foster, I., J. Vockler, M. Wilde and Y. Zhao, 2002. Chimera: A Virtual Data System for Representing, Querying and Automating Data Derivation, Proc. Conf. Scientific and Statistical Database Management, pp: 37-46.
3. Madden, S., J. Franklin, J. Hellerstein and W. Hong, 2002. TAG: A Tiny Aggregation Service for Ad-Hoc Sensor Networks, ACM SIGOPS Operating Systems Rev., 36(SI): 131-146.
4. Lim, H., Y. Moon and E. Bertino, 2010. Provenance-Based Trustworthiness Assessment in Sensor Networks, "Proc. Seventh Int'l Workshop Data Management for Sensor Networks, pp: 2-7, 2010.

5. Simmhan, Y., B. Plale and D. Gannon, 2005. A Survey of Data Provenance in E-Science, ACM SIGMOD Record, 34: 31-36.
6. Muniswamy-Reddy, K., D. Holland, U. Braun and M. Seltzer, 2006. Provenance-Aware Storage systems, Proc. USENIX Ann. Technical Conf., pp. 4-4.
7. Fan, L., P. Cao, J. Almeida and A.Z. Broder, 2000. Summary Cache: A Scalable Wide-Area Web Cache Sharing Protocol, IEEE/ACM Trans. Networking, 8(3): 281-293.
8. Hasan, R., R. Sion and M. Winslett, 2009. The Case of the Fake Picasso: Preventing History Forgery with Secure Provenance, Proc. Seventh Conf. File and Storage Technologies (FAST), pp: 1-14.
9. Garofalakis, M., J. Hellerstein and P. Maniatis, 2007. Proof Sketches: Verifiable In-Netwok Aggregation, "Proc. IEEE 23rd Int'l Conf. Data Eng. (ICDE), pp: 84-89.
10. Sultana, S., E. Bertino and M. Shehab, 2011. A Provenance Based Mechanism to Identify Malicious Packet Dropping Adversaries in Sensor Networks, Proc. Int'l Conf. Distributed Computing Systems (ICDCS) Workshops, pp: 332-338.
11. Kirsch, A. and M. Mitzenmacher, 2006. Distance-Sensitive Bloom Filters, Proc. Workshop Algorithm Eng. and Experiments, pp: 41-50.
12. Rothenberg, C., C. Macapuna, M. Magalhaes, F. Verdi and A. Wiesmaier, 2011. In-Packet Bloom Filters: Design and Networking Applications, Computer Networks, 55(6): 1364-1378.