ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

An Efficient and Secure Method for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks

Vijay Kumar D A
II Year M.Tech (CNE)
Department of Computer Science & Engineering
Dayananda Sagar College of Engineering
Bangalore, India.
vrider00780@gmail.com

Dr. S. Venkatesan
Professor
Department of Computer Science & Engineering
Dayananda Sagar College of Engineering
Bangalore, India.
selvamvenkatesan@gmail.com

Abstract

A Lightweight Secure Scheme for Detecting In computer networking, a packet drop attack or black hole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from a number of different causes. One cause mentioned in research is through a denial-of-service attack on the router using a known DDoS tool. Because packets are routinely dropped from a lossy network, the packet drop attack is very hard to detect and prevent. In Wireless Sensor Networks. Wireless Sensor Network is broadly used in many application domains. These nodes collect data from many sensor nodes. There are many promising attacks like provenance forgery, Packet drop 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. In this paper focus on Provenance Forgery attack, Packet Loss and Detection methods in Wireless Sensor Network.

Keywords: ***Provenance forgery attack, Packet Drop attack, Bloom Filter, RSA.***

Introduction

Sensor networks are used in numerous application domains, such as cyber physical infrastructure systems, environmental monitoring, power grids, etc. 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 (BS) that performs decision-making.

The diversity of data sources creates the need to assure the trustworthiness of data, such that only trustworthy information is considered in the decision process. Data provenance is an effective method to assess data trustworthiness, since it summarizes the history of ownership and the actions per-formed on the data. Recent research [1] highlighted the key contribution of provenance in systems where the use of untrustworthy data may lead to catastrophic failures (e. g., SCADA systems). Although provenance modeling, collection, and querying have been studied extensively for workflows and curated databases [2], [3], provenance in sensor networks has not been properly addressed. 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. In a multi- hop

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

sensor network, 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 constraints of sensor nodes.

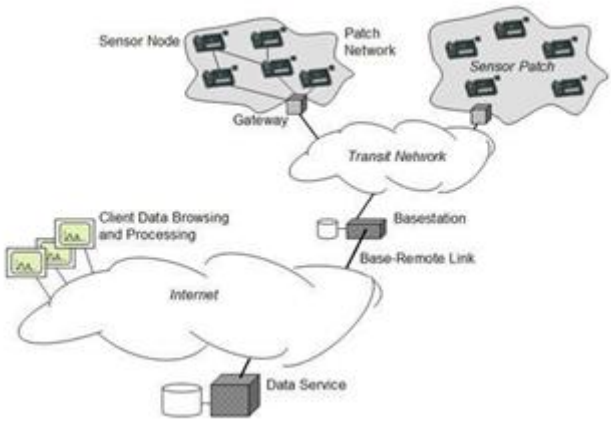
Therefore, it is necessary to devise a light- weight provenance solution with low overhead. Furthermore, sensors often operate in an untrusted environment, where they may be subject to attacks. Hence, it is necessary to address security requirements such as confidentiality, integrity and freshness of provenance. 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.

As opposed to existing research that employs separate transmission channels for data and provenance [4], we only require a single channel for both. Furthermore, traditional provenance security solutions use intensively cryptography and digital signatures [5], and they employ append-based data structures to store provenance, leading to prohibitive costs. In contrast, 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.

Our specific contributions are:

- 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.

SYSTEM ARCHITECTURE:



EXISTING SYSTEM:

- Recent research highlighted the key contribution of provenance in systems where the use of untrustworthy data may lead to catastrophic failures (e.g., SCADA systems). Although provenance modeling, collection, and querying have been studied extensively for workflows and curated databases, provenance in sensor networks has not been properly addressed.
- Pedigree captures provenance for network packets in the form of per packet tags thatstore a history of all nodes and processes that manipulated the packet.
- Hasan et al. propose a chain model of provenance and ensure integrity and confidentiality through encryption, checksum and incremental chained signature mechanism.
- Chong et al. embed the provenance of data source within the data set.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

DISADVANTAGES OF EXISTING SYSTEM:

- Traditional provenance security solutions use intensively cryptography and digital signatures, and they employ append-based data structures to store provenance, leading to prohibitive costs.
- Employs separate transmission channels for data and provenance

PROPOSED SYSTEM:

- 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.

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.

METHODOLOGY

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. The problem of secure provenance transmission in sensor networks proposes an in-packet Bloom filter provenance encoding scheme. Each sensor node generates data periodically, and individual values are routed and aggregated towards the BS using any existing hierarchical dissemination scheme. Each data packet contains a unique packet sequence number, a data value and provenance. The sequence number is attached to the packet by the data source, and all nodes use the same sequence number. The sequence number integrity is ensured through message authentication codes (MAC). To satisfy security and performance, provenance encoding and decoding mechanism were designed. In provenance encoding strategy 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 data, the base station (BS) extracts and verifies the provenance and proposed efficient mechanisms for provenance verification and reconstruction also at the base station.

In Provenance Verification mechanism, the BS conducts the verification process not only to verify its knowledge of provenance but also to check the integrity of the transmitted provenance. The Provenance Collection mechanism verifies the data to ensure its origin, and rejects the data if the verification fails at the base station. This encoding scheme allows the BS to detect packet drop attack organized by a malicious node by binding

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

provenance data with each packet by using Provenance Collection algorithm.

MODULE DESCRIPTION:

Cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of third parties More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering.

Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Key generation

RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.
   - For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.
2. Compute $n = pq$.
   - n is used as the modulus for both the public and private keys
3. Compute $\varphi(n) = (p-1)(q-1)$, where φ is Euler's totient function.
4. Choose an integer e such that $1 < e < \varphi(n)$ and greatest common divisor of $(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are coprime.
   1. e is released as the public key exponent.
   2. e having a short bit-length and small Hamming weight results in more efficient encryption - most commonly 0x10001 = 65,537. However, small values of e (such as 3) have been shown to be less secure in some settings.
5. Determine d as:

$$d \equiv e^{-1} \pmod{\varphi(n)}$$

i.e., d is the multiplicative inverse of e mod $\varphi(n)$.

- This is more clearly stated as solve for d given $(de) = 1 \bmod \varphi(n)$
- This is often computed using the extended Euclidean algorithm.
- d is kept as the private key exponent.

By construction, $d*e = 1 \bmod \varphi(n)$. The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d which must be kept secret. (p, q, and $\varphi(n)$ must also be kept secret because they can be used to calculate d.)

- An alternative, used by PKCS#1, is to choose d matching $de \equiv 1 \bmod \lambda$ with $\lambda = \text{lcm}(p-1, q-1)$, where lcm is the least common multiple. Using λ instead of $\varphi(n)$ allows more choices for d. λ can also be defined using the Carmichael function, $\lambda(n)$.
- The ANSI X9.31 standard prescribes, IEEE 1363 describes, and PKCS#1 allows, that p and q match additional requirements: be strong primes, and be different enough that Fermat factorization fails.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Encryption

Alice transmits her public key $(n, e)$to Bob and keeps the private key secret. Bob then wishes to send message **M** to Alice.

He first turns **M** into an integer m, such that $0 \leq m < n$by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext $c$corresponding to

$$c = m^e \pmod{n}$$

This can be done quickly using the method of exponentiation by squaring. Bob then transmits $c$to Alice.

Note that at least nine values of m could yield a ciphertext c equal to m,[5] but this is very unlikely to occur in practice.

Decryption

Alice can recover $m$from $c$by using her private key exponent $d$via computing

$$m = c^d \pmod{n}$$

Given m, she can recover the original message **M** by reversing the padding scheme.

Sign Module

In sign module following process are preformed. 1. Key generation, 2.encryption, 3.key exchanging 4.signature 5.send to verify module

Provenance Verification

In verify modules following process are preformed. 1. Key generation, 2.decryption, 3.key exchanging 4.send to receiver module

PERFORMANCE ANALYSIS

We use the following benchmarks:

1. We adapt the generic secure provenance framework SProv [5] to sensor networks. In this lightweight version of the scheme, referred to as SSP, we simplify the provenance record at a node n_i as P_i ¼ < n_i hash(D_i), C_i >, where hash(D_i) is a cryptographic hash of the updated data, and C_i contains an integrity checksum as Sign(hash(n_i, hash(D_i | $C_{i\ 1}$).

2. We also consider a MAC-based provenance scheme, referred to as MP, where a node transmits the nodeID and a MAC computed on it as the provenance record.

SIMULATION RESULTS

We implemented and tested the proposed techniques using the NS2 simulator. We consider a network of 39 nodes. First, we look at how effective the secure provenance encoding scheme is in detecting provenance forgery and path changes. Next, we investigate the accuracy of the proposed method for detecting packet loss.

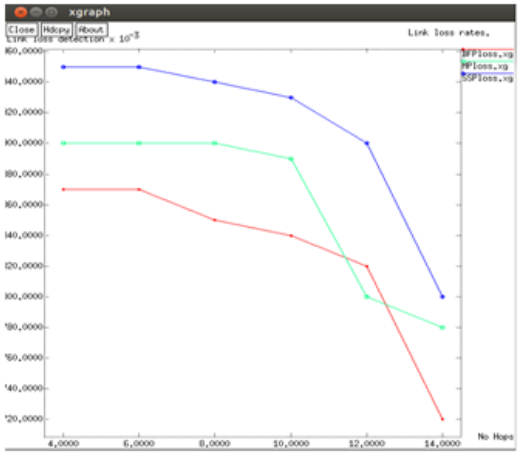


Fig. 1. Link loss detection

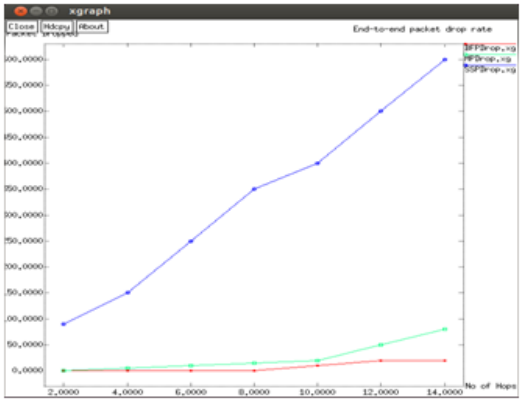


Fig. 2. End – to – End packet drop

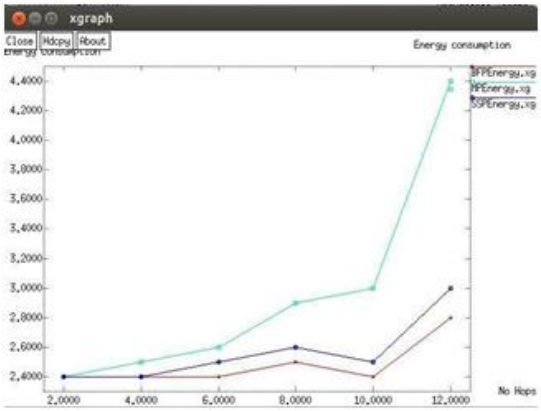


Fig. 3. Energy consumption

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

CONCLUSION

This paper describes the need of provenance data for data transmitted in network and the need of securing this provenance data, extended the scheme to incorporate data-provenance binding and to include packet sequence information that supports detection of packet loss attacks in WSNs. It also shows the various methods to save more energy and bandwidth. This paper goal is to improve the mechanism of provenance in wireless sensor networks by delivering the efficient transmission of secure provenance data along the transmitting medium, free from external threats.

REFERENCES

[1] Salmin Sultana, Gabriel Ghinita, Member, IEEE , Elisa Bertino, Fellow, IEEE , and Mohamed Shehab, Member, IEEE Computer Society, "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, MAY/JUNE 2015.

[2] 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 Manage- ment, pp. 37-46, 2002.

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

[4] Y. Simmhan, B. Plale, and D. Gannon, "A Survey of Data Prove-nance in E-Science," ACM 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," Proc. Seventh Conf. File and Storage Technologies (FAST), pp. 1-14, 2009.

[6] S. Madden, J. Franklin, J. Hellerstein, and W. Hong, "TAG: A Tiny Aggregation Service for Ad-Hoc Sensor Networks," ACM SIGOPS Operating Systems Rev., vol. 36, no. SI, pp. 131-146, Dec. 2002.

[7] K. Dasgupta, K. Kalpakis, and P. Namjoshi, "An Efficient Cluster-ing Based Heuristic for Data Gathering and Aggregation in Sensor Networks," Proc. Wireless Comm. and Networking Conf., pp. 1948- 1953, 2003.

[8] 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, pp. 332-338, 2011.

[9] L. Fan, P. Cao, J. Almeida, and A.Z. Broder, "Summary Cache: A Scalable Wide-Area Web Cache Sharing Protocol," IEEE/ACM Trans. Networking, vol. 8, no. 3, pp. 281-293, June 2000.

[10] A. Kirsch and M. Mitzenmacher, "Distance-Sensitive Bloom Filters," Proc. Workshop Algorithm Eng. and Experiments, pp. 41-50, 2006.

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

[12] M. Garofalakis, J. Hellerstein, and P. Maniatis, "Proof Sketches: Verifiable In-Netwok Aggregation," Proc. IEEE 23rd Int'l Conf. Data Eng. (ICDE), pp. 84-89, 2007.

[13] T. Wolf, "Data Path Credentials for High-Performance Capabili-ties-Based Networks," Proc. ACM/IEEE Symp. Architectures for Net-working and Comm. Systems, pp. 129-130, 2008.

[14] H. Chan, A. Perrig, and D. Song, "Secure Hierarchical In-Network Aggregation in Sensor Networks," Proc. Conf. Computer and Comm. Security (CCS), pp. 278-287, 2006.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[15] 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.

[16] C. Karlof and D. Wagner, "Secure Routing in WirelessSensorNet-works:Attacksand Countermeasures," Proc. Int'l Workshop Sensor Network Protocols and Applications, pp. 113-127, 2003.