Study of Efficient and Reliable Trust Model for Wireless Sensor Nodes

Razi AHMED
Newports Institute of Communications and Economics, Karachi

Mushtaq HUSSAIN
Newports Institute of Communications and Economics, Karachi

Raheel IQBAL
Muhammad Ali Jinnah University

Muhammad Ali PERACHA
University of Karachi

Muhammad Liaquat ALI
University of Karachi.

Abstract

Trust model in Wireless Sensor Network (WSN) is the primary concern for researchers. Intrusion detection with limited constraints is the main study of my research. Wireless sensor consumes lots of power and cost to detect intruder. My research is based on how to minimize this cost and how to efficiently and reliably captured the intruder in Trust model. I have developed a trust model for Wireless Sensor Network in which intrusion detection is faster than previous models.

Keywords

Trust Model, Intrusion Detection, Efficient Intrusion detection.

1 Introduction

Wireless Sensor Networks (WSN) have been proven a useful technology for perceiving information about the physical world and as a consequence has been used in many applications such as measurement of temperature, radiation, etc. The nature of this kind of technology, and also their vulnerabilities to attacks make the security tools required for them to be considered in a special way. The decision making in a WSN is essential for carrying out certain tasks as it aids sensors establish collaborations. In lodge to help this process, trust management systems could meet a relevant part.

To overcome the shortcoming of cryptographic-based secure data-aggregation, reputation and trust schemes are being produced to complement existing technologies for monitoring network activities and outcomes. Reputation and trust systems are utilized to detect, collect, process, and disseminate feedback concerning the sensors' recent behaviors and to assess their trustworthiness for specific applications. The goals of utilizing such arrangements are to defend against node capture attack that results in the occurrence of compromised nodes, identified nodes that have been compromised, and eject them from further participation in data-collection. The trustworthiness of sensors is evaluated based on their various activities, including data collection, data transmission, aggregator selection, and routing path selection. The reputation of each node refers to the expectation of neighboring nodes concerning a node's behavior based on their observations of its past actions. Hence, trust and reputation in a WSN often are observed together. Thus, a node's expectation will affect its choices and actions. The confidence of a

node generally is determined as the expected value of that node's reputation.

2 Related Works

There were so many techniques to the identify malicious node in a wired network, but it cannot be implemented in wireless network due to limited resources and energy. Wireless sensor network has been studied in a number of researches. Lee was the first researcher who studied in the wireless sensor network and identify the problem of Wireless sensor network. He suggested the architecture for cooperative intrusion catching mechanism and also suggested the architecture for distributed intrusion catching mechanism. His scheme totally based on statistical theory of intrusion detection. But his scheme takes much data, traffic and time to detect intrusion. wireless sensor network the is a costly affair as such cannot be afforded.

Xi Peng explored for wireless sensor trust model and proposed a security model for WSN. Later on his proposed model which detect lots of intruders. Byunggil Lee has projected a security model for wireless sensor network. Qi wanghassuggested detection algorithm for WSN in a low complexity network.

3 Methodology

To reduce the cryptographic work at each sensor node while preventing malicious packets from infecting large portions of the network, we introduce a cooperative mechanism where nodes cooperate in checking malicious incoming packets. By sustaining a number nodes checking in every pointing time and making them cooperate, expensive homomorphic hashing can be used less frequently, hence, improving the functioning of the network. Supplementing the details of how such efficient mechanism works. Its assumed that nodes

check blocks with probability. Encoded packets that pass the check are marked as safe, while encoded packets that have not even been checked are kept in an insecure window. Encoded packets are checked in batches. The batch window is equal to the insecure window. Whenever a node verifies its insecure window, valid encoded packets are labelled as safe and the insecure window is reset. One possible solution to improve computation time is to verify encoded packets in batches, either probabilistically or periodically. In such solution nodes do not check every encoded packet, but they check a window of encoded packets all at once. Batching is possible thanks to the homomorphic properties of the hashing functions.

A hash function, say hi (.), maps a large input, which is a block of information, say b, to an output h (b) typically of much smaller size. Function h(b) has the important property that given b it is difficult to find another input block b^0 with the same hash value $h(b^0) = h(b)$. Homomorphic hash functions have the additional property that the hash value of a linear combination of some input blocks can be constructed efficiently by a combination of the hashes of the input blocks. More specifically, if the original blocks are b_i, with [1,n],then the hash value of the linear combination $b' = c_1b_1 + c_2b_2 + \ldots + c_nb_n$ is $h(b') = h^{c1}(b_1), h^{c2}(b_2),\ldots,h^{cn}(b_n)$. We prove that property in Lemma below.

Here, each block b_i is divided into m codewords $b_{k;i}$, k = 1 . . . m. Before computing the hash of a block we need to decide on the hash parameters G = (r,q,g). The parameters r and q are prime numbers of order and chosen such that q /(r-1).

The parameter g is a vector of m numbers such that each of the elements of the vector can be written as $x^{(r-1)/q}$, where X Zq and x 1. ≠ The number of code words m is such that each element is less than . More details about the sizes of the prime numbers r and q and

algorithms for the efficient construction of G can be found in Table I

Table I
Homomorphic Hashing Function Parameters

Name	Description	e.g.
r	discrete log security parameter	1024 bit
q	discrete log security parameter	257 bit
r	random prime jrj = r	
q	random prime qj(r 1); jqj = q	
m	number of "sub-blocks" per block	512
g	1 m row vector of order q in Z_q	
	block size	16 KB

We define a hash for each block $b_i = [b_{1,i} b_{2,i}, \ldots b_{m;;i}]$ as

$$h(b_i) \quad \prod_{k=1}^{m} g_k^{b_{k,i}} \bmod p$$

The hash of the file F is simply the vector of the hash of each b_i:

$$H(F) = (h(b_1), h(b_2), \ldots, h(b_n))$$

Whenever a node first joins the system, it downloads from the server the hash of the file H(F) as well as the security parameters G. This hash will be used to check encoded blocks on-the-fly [element in hashs are elements in (typically 128 bytes long), which is 1/128 times the size of block of size 16kb.]

We now show that the hash of an encoded block can be

constructed by the hashes of the original blocks. Hence, it is possible to check whether a received encoded block and coefficient vector are indeed correct.

Lemma: (Homomorphic hashing for network coding):

The hash value of the encoded block $e = \sum_{i=1}^{n} c_i b_i$ can be computed by the hashes of the original blocks:

$$h(c) - \prod_{i=1}^{n} h^{ci}(b_i) \bmod p$$

Proof: Assume an encoded block $e = \sum_{i=1}^{n} c_i b_i$ all arithmetic operations are in the Zp field. The hash of this block is

$$h(e) \quad h(\sum_{i=1}^{n} c_i b_i)$$

$$= \prod_{k=1}^{m} g_k^{h(\sum_{i=1}^{n} c_i b_i) \bmod q} \bmod r$$

Observe that the sum in the exponent can be written as

$$\sum_{i=1}^{n} c_i b_{k,i} \quad q.quot + (\sum_{i=1}^{n} c_i b_{ki}) \bmod q$$

Where quot is the quotient of dividing $\sum_{i=1}^{n} c_i b_{k,i}$ by q. and, hence. $g_k^{h\sum_{i=1}^{n} c_i b_{ki}} \bmod r$ can be written as $(g_k^{(\sum_{i=1}^{n} c_i b_{ki}) \bmod q} \bmod r)$

Recall $g_k = x_k^{(r-1)/q}$ the, and form Fermat's little theorem,

$$g_k^{q \cdot quot} \bmod r \quad (g_k^{(r-1)} \bmod r)^{quot} \bmod r = 1$$

Thus, h(e) can be expressed as

$$\prod_{k=1}^{m} g_k^{\sum_{i=1}^{n} c_i b_i} \bmod r \quad \prod_{k=1}^{m} \prod_{i=1}^{n} (g_k^{b_{ki}})^{c_i} \bmod r$$

$$\prod_{i=1}^{n} (\prod_{k=1}^{m} g_k^{b_{ki}})^{c_i} \bmod r$$

$$- \prod_{k=1}^{m} h(b_i)^{c_i} \bmod r$$

Those nodes that downloaded incoming packets encoded with insecure window encoded packets, and those nodes that delivered the encoded packets inside the insecure window. Alert messages are propagated from one node to another until all infected nodes are informed. If the insecure window is empty, alert messages are not processed. Alert messages are processed as soon as they are received. However, alert messages are only propagated after the node is convinced that a malicious encoded packet exists. Duplicated alert messages can be received in the same malicious packet since overlays often contain loops. However, such duplicated messages will be discarded when

- The insecure window is empty,
- The duplicate message comes from a sensor node that is not on the insecure activity table. In addition to alerting its neighbors, a sensor node takes the following actions:

- it puts encoded packets in the insecure window in isolation to be checked and cleaned in the background,

- it stops using encoded packets in the insecure window for network coding, and

- it starts checking encoded packets with probability one until the insecure window is secured and cleaned, thus, preventing new malicious incoming packets from infecting the reprogramming system.

4 Conclusion

An improved data collection method for WSNs is presented in this report. The method is reliable, trust-based, energy-efficient, and safe. The cryptographic and links availability, to improve trust-based data-collection. Introducing residual energy and link availability facilitates the reputation system's ability to keep aggregators and nodes in the routing path from being used excessively and guarantees that the routing path selected by the reputation system will be much more reliable. In summation, the recovery mechanism prevents compromised node's child nodes from being set apart and helps those nodes to reselect new parent clients. Simulation results indicated that the proposed cryptographic with respect to its improved performance of data accuracy path reliability, and the lifetime of data-aggregation, while cutting down energy use. Therefore, the proposed cryptographic achieved its goal of maintaining good data-aggregation in WSNs more reliable and energy-effective.

References:

[1]. A. Milenković, C. Otto, and E. Jovanov, "Wireless sensor networks for personal health monitoring: issues and an implementation," Computer Communications, vol. 29, no. 13-14, pp. 2521-2533, 2006.View at Publisher · View at Google Scholar · View at Scopus.

[2]. K. Akkaya, M. Demirbas, and R. S. Aygun, "The impact of data aggregation on the performance of wireless sensor networks," Wireless Communications and Mobile Computing, vol. 8, no. 2, pp. 171-193, 2008. View at Publisher · View at Google Scholar · View at Scopus.

[3]. R. Rajagopalan and P. K. Varshney, "Data aggregation techniques in sensor networks: a survey," IEEE Communications Surveys and Tutorials, vol. 8, no. 4, pp. 48-63, 2006.

[4]. S. Ozdemir and Y. Xiao, "Secure data aggregation in wireless sensor networks: a comprehensive overview," Computer Networks, vol. 53, no. 12, pp. 2022-2037, 2009. View at Publisher · View at Google Scholar · View at Scopus

[5]. S. Ozdemir, "Functional reputation based data aggregation for Wireless sensor networks," in 4th IEEE International Conference on Wireless and Mobile Computing, Networking and Communication (WiMob '08), pp. 592-597, October 2008. View at Publisher · View at Google Scholar · View at Scopus

[6]. S. Ozdemir, "Functional reputation based reliable data aggregation and transmission for wireless sensor networks," Computer Communications, vol. 31, no. 17, pp. 3941-3953, 2008. View at Publisher · View at Google Scholar · View at Scopus

[7]. A. Boukerche and Y. Ren, "A trust-based security system for ubiquitous and pervasive computing environments," Computer Communications, vol. 31, no. 18, pp. 4343-4351, 2008. View at Publisher ·View at Google Scholar · View at Scopus

[8]. Y. Ren and A. Boukerche, "Modeling and managing the trust for wireless and mobile ad hoc networks," in IEEE International Conference on Communications (ICC '08), pp. 2129-2133, Beijing, China, May 2008. View at Publisher · View at Google Scholar · View at Scopus

[9]. S. Ganeriwal and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," inProceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04), pp. 66-77, October 2004. View at Scopus

[10]. S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," ACM Transactions on Sensor Networks, vol. 4, no. 3, article 15, 2008. View at Publisher · View at Google Scholar · View at Scopus

[11]. R. A. Shaikh, H. Jameel, S. Lee, S. Rajput, and Y. J. Song, "Trust management problem in distributed wireless sensor networks," in 12th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA '06), pp. 411-414, Sydney, Australia, August 2006. View at Publisher · View at Google Scholar · View at Scopus

[12]. P. Michiardi and R. Molva, "CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc network," in Proceedings of the IFIP Conference on Communications and Multimedia Security, vol. 228, pp. 107-121, Portoroz, Slovenia, 2002.

[13]. A. Srinivasan, J. Teitelbaum, and W. Jie, "DRBTS: distributed reputation-based beacon trust system," in2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC '06), pp. 277-283, Ind, USA, October 2006. View at Publisher · View at Google Scholar · View at Scopus

[14]. A. Jøsang and R. Ismail, "The beta reputation system," in Proceedings of the 15th Bled Conference on Electronic Commerce, p. 41, 2002.