Journal of Network and Computer Applications 59 (2016) 88–94

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

BTRES: Beta-based Trust and Reputation Evaluation System for wireless sensor networks

Weidong Fang [a,c], Chuanlei Zhang [b,*], Zhidong Shi [a], Qing Zhao [b], Lianhai Shan [c,d]

[a] Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Shanghai University, Shanghai 200444, China
[b] School of Computer Science and Information Engineering, Tianjin University of Science & Technology, Tianjin 300222, China
[c] Key Laboratory of Wireless Sensor Network & Communication, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200051, China
[d] Shanghai Research Center for Wireless Communications. Shanghai 200335, China

ARTICLE INFO

Available online 7 July 2015

Keywords:
WSNs
Trust evaluation
Beta distribution
Compromised nodes

ABSTRACT

Unlike traditional networks, the wireless sensor networks (WSNs) are very vulnerable to internal attacks from compromised nodes. The trust management system is the most effective way to defend the attack inside the network. The Beta-based Trust and Reputation Evaluation System (BTRES) is proposed in this paper for WSNs' node trust and reputation evaluation. BTRES is based on monitoring nodes' behavior, and beta distribution is used to describe the distribution of nodes' credibility. The node trust values are used to guide the selection of relay nodes, mitigating internal attacks risks. Simulation results show that the use of BTRES could effectively maximize the defense of internal attacks from compromised nodes and improve the WSNs' information security. In this paper, we mainly focus on the communication trust and data trust, and energy trust can be easily integrated into BTRES.

1. Introduction

Wireless Sensor Networks (WSNs) is widely used in military, industrial, agriculture and commercial fields. The security of WSNs is an important issue and they are getting more and more attention (Prathap et al., 2012). WSNs security issues in certain applications will cause economic loss and privacy issues. Therefore, WSNs security has become a hot research topic recently (Shashikala and Kavitha, 2012).

The cheap WSNs node, which is deployed in the local area, can easily be captured and attacked. What is more, due to the limitation of nodes' energy, computing and storage capability, it easily leads to a node failure or low competitiveness of selfish nodes. The attacks to WSNs are from external attacks and internal attacks. The traditional encryption and authentication schemes are mainly used against external attacks (Li et al., 2013, 2011; Meena and Jha, 2015). However, once a node is captured, it could cause key leak very easily, which cause encryption and authentication schemes failure. Therefore, for the purposes of defense against internal attack, current encryption and authentication schemes cannot satisfy WSNs' security requirements. How to defend the attack from compromised nodes or problematic nodes becomes one of the major directions in WSNs security mechanism research.

At present, the most effective way to defend internal attack is trust management system. The trust management systems are divided into three categories: trust model, trust management scheme and protocol optimization.

In terms of the trust model, Ganeriwal and Srivastava (2004) proposed a reputation-based framework for high integrity sensor networks (RFSN). This framework included five sections: direct reputation evaluation, indirect reputation evaluation, reputation synthesis, conversion and node behavior trust, which gave a complete evaluation of the general process of sensor nodes trust. Then, based on the Beta distribution and Bayesian formula, the Beta Reputation-system for Sensor Networks (BRSN) was proposed. The feasibility of Beta distribution was verified by derivation and detailed explanation of calculations for the reputation of the update, aging, indirect information and trust were elaborated. BRSN was a simple trust evaluation system and it has been widely studied and used. Jiang et al. (2015) proposed the Efficient Distributed Trust Model (EDTM) for WSNs. In this model, according to the number of packets received by sensor nodes, direct trust and recommendation trust were selectively calculated. Communication trust, energy trust and data trust were considered during the calculation of direct trust, and trust reliability and familiarity were defined to improve the accuracy of recommendation trust. Sinha and Jagannatham (2014) proposed the Gaussian trust and reputation for fading Multiple-Input Multiple-Output (MIMO) WSNs. Based on multivariate Gaussian distribution and Bayesian theorem, considering the impact of the MIMO wireless fading

* Correspondence to: 1038, Da Gu Nan Lu, 300222, Tianjin, China. Tel.: +8602262070083.
E-mail address: a17647@gmail.com (C. Zhang).

http://dx.doi.org/10.1016/j.jnca.2015.06.013
1084-8045/

channel, the authors combined the direct and indirect reputation information. The reputation and trust value was also calculated. This method could effectively isolate the malicious node, but the calculation process was too complex for energy-limited WSNs. There were some other representative researches. Zhang et al. (2010) put forward a dynamic trust establishment and management framework for WSNs. On basis of the previous trust management system of WSNs, some new measurements (for example, nodes only communicate with the cluster head and use cluster head trusted information.) were considered, which made the trust management system better. Zhu et al. (2010) put forward a Rank-based Application-driven Resilient Reputation framework Model for wireless sensor networks (RARRM). The model was application-driven and different requirements could have different trust value rank.

For the purposes of trust management scheme, Yu et al. (2010) summarized the Trust and Reputation Management (TRM) systems in wireless communication systems. The authors divided the existing TRM systems into two categories: individual-level trust models and system-level trust models. Individual-level trust models mainly focused on the trust evaluation of one node to another node; but the system-level trust models included trust and reputation evaluation model and protocol, where reward and punishment were made based on the node's reputation. Through the examples of the major individual level model, the author introduced the trust and credibility of the initial stage, evaluated the reputation of the direct and indirect aspects of synthesis and guided trust evaluation and decision-making. The authors also presented several reward and punishment mechanism for system-level trust model. At last, the advantage and disadvantage of TRM systems were summarized. Duan et al. (2014) proposed the trust derivation scheme based on game theory. At first, the authors analyzed the network security requirements and mechanisms. Then, under the premise of ensuring network security, a risk model was exhibited to stimulate the cooperation of WSNs node to derive an optimal number of cooperating nodes. At last, the game theoretic approach was applied to the trust derivation process to reduce the overhead of the process. Li et al. (2013) proposed a Lightweight and Dependable Trust System (LDTS) for clustered WSNs. Firstly, the author proposed a lightweight trust decision scheme based on node identity clustering of WSNs. Then, by eliminating feedback between cluster members and Cluster Heads (CHs), the system efficiency was greatly improved and the harm of malicious nodes was reduced. At last, because of the significance of cluster head which undertakes a lot of data transition tasks, a trust evaluation method was defined for interaction of CHs. What is more, an adaptive weighting method was defined. Hui-hui et al. (2009) summarized the trust evaluation in WSNs as: communication trust, data trust and energy trust. Communication trust meant the relationship value calculated between two cooperation nodes in a wireless sensor network which can send or receive information from each other. Data trust refered to the trust assessment of the fault tolerance and consistency of data. Energy trust in WSNs refered to the relationship between the remaining energy of a node and the energy threshold necessary to complete a new communications and data-processing tasks. In addition, Li et al., (2010) presented a data-centric trust evaluation mechanism in WSNs (DTSN). Because WSN was a data-centric network, the traditional trust evaluation based on entities could not apply to WSNs. Shaikh et al. (2009) proposed a group-based trust management scheme for clustered WSNs. In this trust management scheme, energy consumption was considered firstly. The approach reduced the cost of trust evaluation. Zia and Islam (2010) presented a solution based on Communal Reputation and Individual Trust (CRIT) for WSNs. The nodes' behaviors were monitored by a watch dog, and each node had a trust table and a reputation table for its adjacent nodes. Ukil (2010) proposed a trust and reputation based collaborating computation, and the optimum path could be chosen by this scheme. Ishmanov and Kim (2011) presented a secure trust establishment for WSNs. Unlike traditional trust evaluation mechanism, this mechanism only considered the impact of the abnormal node behavior. Bao et al. (2011), (2012) proposed the trust-based intrusion detection and a hierarchical trust management for WSNs which is applied to trust-based routing and intrusion detection. In addition, the selection of minimum trust threshold was also analyzed, where Zhu et al. (2014) built a trust and reputation management system for cloud and sensor networks integration.

In protocol optimization, Gheorghe et al. (2013) proposed an Adaptive Trust Management Protocol (ATMP) based on intrusion detection. The ATMP, which was applied to TinyOS system, could defend varous kinds of attack with combination of TinyAFD common intrusion detection framework. The protocol included three phases: (1) Learning phase, in which experience was computed based on these alerts received from TinyAFD, (2) exchanging phase, in which experience associations were exchanged between neighbor nodes and (3) updating phase, in which trust and reputation were updated based on experience. This protocol was simple and could only be applied in TinyOS system. But it did not take into account the node residual energy problems. According to the sensor nodes' behaviors on event perception, packet forwarding and data aggregation, Fang et al. (2013) proposed a reputation management scheme, which described the initialization, update, and storage of the reputation value and the punishment and redemption of malicious nodes. When the scheme was applied to the Security Privacy In Sensor Network (SPIN) protocol, a new trust enhanced routing protocol based-on reputation was propose the results of the simulation indicated that the trust enhanced routing protocol improved the data forwarding rate and delivery success rate in distrusted environment for WSNs. Tajeddine et al. (2011) put forward a centralized TRust And Competence-based Energy-efficient routing scheme for wireless sensor networks (TRACE). In TRACE, using centralized management of sinks made routing more efficient and secure. On this basis, Tajeddine et al. (2012) proposed a CENtralized Trust-based Efficient Routing protocol for wireless sensor networks (CENTER). In the protocol, the BS calculated different quality metrics - namely the maliciousness, cooperation, compatibility and approximation of the battery life, which could evaluate the Data Trust and Forwarding Trust values of each node. Then, the BS used an effective technique to isolate all “bad” nodes, which was misbehaving or malicious based on their history. At last, the BS used an efficient method to disseminate updated routing information, indicating the uplinks and the next hop downlink for each node. Others include: Li et al. (2015) proposed a new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity. Gerrigagoitia et al. (2012) proposed a new IDS design based on reputation and trust of the different nodes of a network for decision-making and analysis of possible sources of malicious attacks. Arijit (2010) put forward a trust and reputation based collaborating computing model. The detection of malicious nodes along with trust and reputation analysis of WSNs made this model robust and secure.

The trust management system has been developed for many years. The definitions of trust and credibility are dependent on the specific application (Momani 2010). In WSNs, the trust generally refers to the reliability of forecasting future behavior of one node to another one. Trust generally is a fixed value. Whether two nodes interact or not is decided by the trust value. On the other hand, although BRSN has been widely studied and used, it only defend several classical internal attacks, such as black hole attack, Sybil attack, and so on. In this paper, based on the interaction of nodes and beta distribution, we propose the Beta-based Trust and Reputation Evaluation System (BTRES) to guide the interaction of