Journal of Ambient Intelligence and Humanized Computing
https://doi.org/10.1007/s12652-018-0949-2

ORIGINAL RESEARCH

Security authentication technology based on dynamic Bayesian network in Internet of Things

Qing Zhang[1,2] · **Dilong Xu**[3]

Received: 31 May 2018 / Accepted: 19 July 2018

Abstract
With the rapid development of the Internet of Things (IoT) technology in the information society, how to meet the urgent requirements of current users for trusted transmission services is a research hot-spots in the field of the IoT industry. In view of the research status on security authentication in IoT, a security authentication technology based on dynamic Bayesian network combined with trusted protocol is proposed in this paper. Through the introduction of the trusted measurement and the combined public key-based security authentication mechanism in the network, it enhances the security information exchange and considers the node credibility and the path reliability in the routing decision so as to choose a high secure and trusted path for information transmission in IoT. The evaluation results showed that our algorithm achieves a much better security performance than comparison algorithms in overhead and computational complexity for real time applications. In addition, our algorithm has also an adaptive capability and can quickly react to the denial of the service attack, which effectively suppress the threat of abnormal entity in the IoT.

Keywords Internet of Things · Dynamic Bayesian network · Security authentication · Trusted transmission · Combined public key · Security information exchange

1 Introduction

With the rapid development of the Internet of Things (IoT) technology in the information society, network security has become the focus of attention in the field of communication networks (Wang et al. 2016). On the one hand, attacks against network nodes are endless and destructive in recent years. Network nodes are exposed to risks such as being attacked and deceived. On the other hand, most researches on information transmission services in the past were based on the ideal conditions of safe and reliable network environment (Xiao and Liu 2017). It is difficult to meet the urgent requirements of current users for trusted transmission services. Therefore, secure routing protocols have become one of the research hot-spots in the field of the IoT industry (Sun et al. 2017).

The IoT is a novel paradigm that aims to bridge the gap between the physical world and its representation in the digital world (Ndibanje et al. 2014). IoT is expected to become an integrated part of the Internet in the future. IoT is defined as a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols. Bandwidth and storage are no longer considered restricting factors in IoT applications because of the rapid development of novel information and communication technologies (Kothmayr et al. 2013). The main issue is how to achieve the trusted transmission services for IoT applications.

Research on secure routing protocols includes two aspects: node security and information interaction security between nodes. The main solutions for current node security include identity authentication and trusted metrics technology based on trusted roots (Park and Kang 2015). The former uses the Trusted Platform Module (TPM) (Gang et al. 2011; Zhao 2013) as a built-in trusted root, and it is used as a starting point, combined with security start-up, data storage protection, integrity metrics, and trusted transitive, which performs step-by-step metrics, verification, and delivery to complete the node's trusted assessment. The disadvantages are: the granularity is relatively coarse and it is difficult to

✉ Qing Zhang
zhangqingls@qq.com

[1] Hunan University, Changsha 410006, Hunan, China

[2] Hunan City University, Yiyang 413000, Hunan, China

[3] Guangzhou Academy of Social Sciences, Guangzhou 510410, Guangdong, China

Published online: 27 July 2018

effectively deal with internal attacks. For example, the Basic Input Output System (BIOS) is easily tampered, resulting in the credibility of the trusted root can not be guaranteed; On the basis of social relations, the latter makes a trusted measurement of the identity and interactive behavior of the node by evidence theory, probability theory etc, but it still needs to be optimized in the aspects of computational complexity, precision and dynamic adaptability.

Internet of Things (IoT) is a network of sensors, actuators, mobile and wearable devices, simply things that have processing and communication modules and can connect to the Internet. In a few years' time, billions of such things will start serving in many fields within the concept of IoT. Self-configuration, autonomous device addition, Internet connection and resource limitation features of IoT causes it to be highly prone to the attacks. Denial of Service (DoS) attacks which have been targeting the communication networks for years, will be the most dangerous threats to IoT networks. Aris et al. proposed a comparison model to analyze and classify the DoS attacks that may direct at the IoT environments and try to detect and mitigate the DoS attacks to IoT will be evaluated (Aris et al. 2015). Most of the information interaction security between nodes are to adopt the cryptography-based security methods. For example, literature (Ammireddy 2017) proposes to use the signature technology to ensure the security of the Open Shortest Path First (Open_SPF) protocol that is a dynamic, hierarchical routing protocol designed to support routing in TCP/IP networks. The Open_SPF routing protocol is a collection of interrelated algorithms (Wu et al. 2017; Tamboli and Dambawade 2017; Bamasag and Toumi 2016; Teng et al. 2017; Griffin 1992). It can effectively resist external attacks, but it is difficult to effectively deal with internal damage, and most of them rely on the support of third-party authentication systems, and it is difficult to meet the needs of large-scale applications.

In view of the research status on security authentication in IoT, a security authentication technology based on dynamic Bayesian network combined with trusted protocol is proposed in this paper. Through the introduction of the credibility and the combined public key (CPK)-based security authentication mechanism in the network, it enhances the security information exchange and considers the node credibility and the path reliability in the routing decision so as to choose a high secure and trusted path for information transmission in IoT.

The rest of this paper is organized as follows: the node trusted metric model is presented in Sect. 2. The Sect. 3 is dedicated to introduction of the main contributes of the study about how to improve the security performance in the IoT, and the improved security authentication technology is developed. The experimental results are presented in Sect. 4. The paper ends up with conclusions and perspectives.

2 Node trusted metric model

The identity authentication based on trusted root is combined with the trusted measurement technology, where the composition and calculation model of trusted measurement are studied (Zhang et al. 2016).

2.1 Composition of trusted measurement model

Trusted Platform Module (TPM) is the key part of Trusted computing platform. There are many keys being managed in TPM, and TPM uses these keys to achieve it's functions, such as security storage, Integrity Measurement, Storage and Reporting. At physical and acquisition level, the security must ensure, at one side, that the nodes would not be cheated, controlled or damaged and, on the other side, that information would not be distorted, faked or replied illegitimately. At the transmission level, security should guarantee the confidentiality, the integrity and the authenticity in data exchange and at application level, it has to ensure the privacy, confidentiality, as well as the safety storage of information so as to cover individual privacy protection, middleware safety, etc. Usually the management of security is carried out by means a model where users within a domain are naturally mapped to roles and access rights are associated with these roles. So many researches are done for enhancing security performance, where the trusted measurement module is a very effective network security model. The composition of the trusted measurement model is shown in Fig. 1, which mainly includes the following modules.

1. Trusted platform module (TPM): Trusted platform module provides authentication, password operation, storage protection and interface services for nodes.
2. Trusted measurement module: Storage and strategy library: Complete the storage of related information and strategy.
3. Trusted cognition module: Complete information collection, data processing and standardized representation. The security, availability, reliability and other basic data of the adjacent nodes are obtained without affecting the performance of the network, and are processed and quantized into a dimensionless value on the interval [0, 1].
4. Mathematical module of trusted measurement: A mathematical model is to complete the calculation of trusted measurement.
5. Trusted decision module: Guide subsequent evidence collection and maintain the list of local trusted relationships.
6. Trusted management module: Complete the management of other modules.

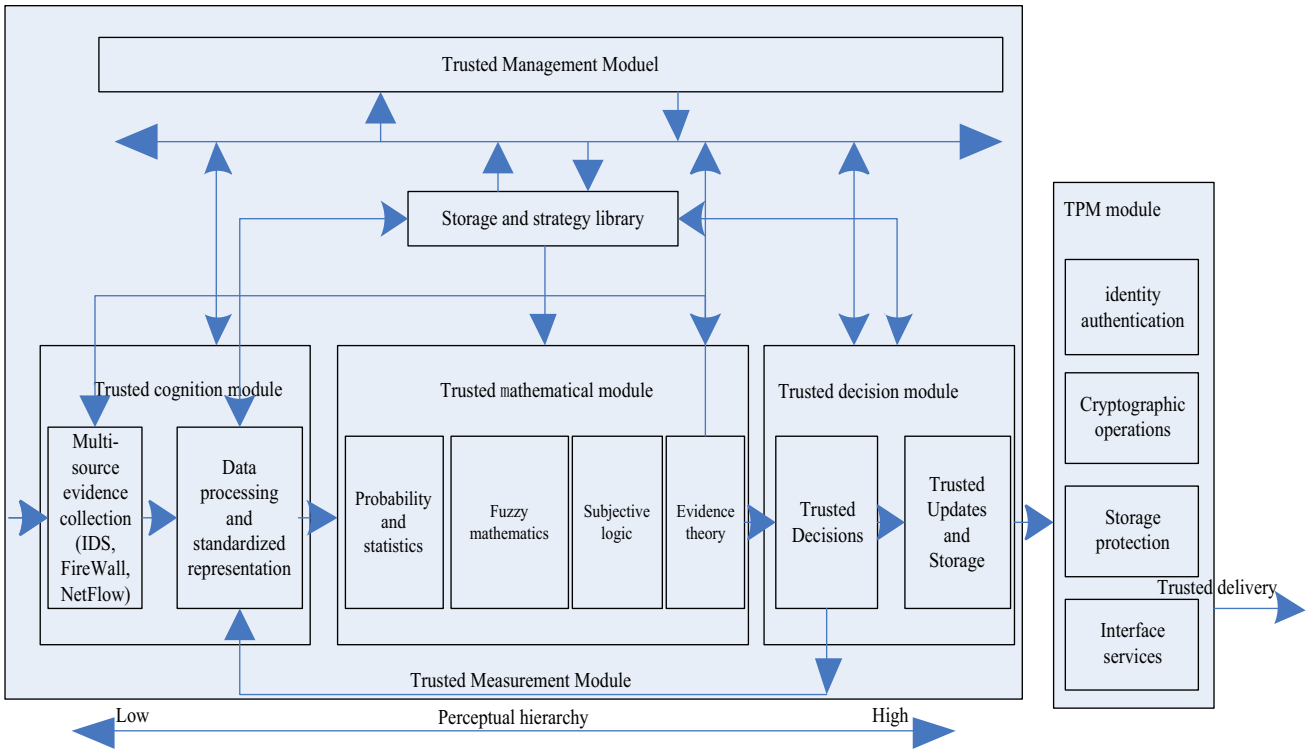

Fig. 1 Trusted measurement model

The TPM module is used to complete the identity authentication and integrity assessment of the nodes, and the trusted measurement module is used to complete the trusted measurement of the node behavior. The combination of the two modules can provide the security assurance with a finer granularity (Wang et al. 2012).

2.2 Computation of trusted measurement model

Definition 1 $G = (V, E, T)$ represents the trusted graph in the current network, where V and E are the set of nodes and edges, respectively. If $\forall\ v_i, v_j \in V$ and $v_i \neq v_j$, we can get $E(v_i, v_j) = E_{ij} \neq \boldsymbol{\Phi}$, $E_{ij} \in E$ and $\mathrm{E}_{ij} \neq E_{ji}$. E_{ij} is the trusted relation of node v_j established by v_i. $T = \{T_1, T_2, \ldots, T_n\}$ is denoted as the set of the trusted measurement.

The comprehensive trusted measurement T_{ij} of node v_i to v_j is computed from its direct trusted measurement D_{ij} and indirect trusted measurement T_{ij}. Its equation is written as follows:

$$\mathrm{T}_{ij}(E_{ij}, C(W_{ij}, t), t) = \begin{cases} I_{ij}(E_{ij}, C(W_{ij}, t), t) & C(W_{ij}, t) = \Phi \\ D_{ij}(E_{ij}, C(W_{ij}, t), t) & C(W_{ij}, t) = C(W, t) \\ T_{ij}(E_{ij}, C(W_{ij}, t_0), t_0)\tau(t) & \Delta C = \Phi \\ \varphi(\alpha_1 D_{ij}(I_{ij}(E_{ij}, C(W_{ij}, t), t) + \alpha_2(I_{ij}(E_{ij}, C(W_{ij}, t), t))), & others \end{cases} \tag{1}$$

where t and t_0 are the current time-stamp and the time-stamp of the trusted calculation finished in the last time; W represents the evidence window with valid interaction; W_{ij} represents the valid evidence of the node v_j collected by the node v_i in W; $\mathrm{C}(W_{ij}, t)$ represents the interaction context of node v_j collected by node v_i before the time-stamp t; $\Delta\mathrm{C} = C(W_{ij}, t) - C(W_{ij}, t_0)$; α_1 and α_2 denote the weights of the direct and indirect trusted measurement, respectively, and $\alpha_1 + \alpha_2 = 1$; $\mathrm{T}_{ij}(E_{ij}, C(W_{ij}, t), t)$ is the integrated trusted measurement of node v_j on v_i in the case of a valid interaction evidence with a time-stamp t, and $\mathrm{T}_{ij}(E_{ij}, C(W_{ij}, t), t) \in [0, 1]$. $\tau(t)$ is the attenuation factor for the trusted measurement, which can be denoted as

$$\tau(t) = 1 - (t - t_0)\delta/t \tag{2}$$

where $\tau(t) \in (0, 1)$; δ is an attenuation adjustment factor, and its value is related to the speed of effective evidence updating, and δ also determines the attenuation speed of trusted measurement. When $\delta = 0$, it does not decline; the larger

the value of δ, the faster the decay. The equation for φ is written as follows:

φ is the penalty factor of the trusted measurement;

$$\varphi = \begin{cases} 1, & \Delta T_i \geq 0 \\ 0 < \varphi < 1, & \Delta T_i < 0 \end{cases} \tag{3}$$

where $\varphi \in (0, 1)$, $\Delta T_i = T_i(t) - T_i(t_0)$. When $\Delta \mathrm{T}_i < 0$, this node needs to be punished, and the smaller φ, the more severe the penalty. The equation for T is written as follows:

$$T_i = \left(\sum_{j=0}^{n} T_{ji} \right) / n \tag{4}$$

where $\mathrm{T}_i \in [0, 1]$, n is the number of node v_i with interactive relationship in network G.

Nowadays, there are many mathematical models for trusted metrics. In this paper, the Trusted Measurement Model based on Dynamic Bayesian Networks is proposed, which uses Bayesian formula and Bayesian theorem as the theoretical basis, the traditional Bayesian network is combined with the time series to define the a priori network, transfer network and conditional probability; On the basis of new evidence acquisition, iterative calculation of the node's comprehensive trusted measurement is realized. Its expression is written as follows:

$$\begin{aligned} \mathrm{T}_{ij}(E_{ij}, C(W_{ij}, t), t) = N(B_{t_0}, B_{\rightarrow}, P(t_0), \ldots \\ T_{ij}(E_{ij}, C(W_{ij}, t_0), t_0), C(W_{ij}, t)) \end{aligned} \tag{5}$$

where N denotes a dynamic Bayesian network mathematical model, $\mathrm{B}_{t_0}, B_{\rightarrow}, P(t_0)$ represents the priori network, transfer network and conditional probability in the times-tamp t, respectively.

3 Secure link state routing protocol

Based on the standard Open_SPF, a trusted transformation is implemented, which introduces a trusted computation and a CPK-based security authentication mechanism to realize a secure link state routing protocol (SLSRP) (Sun and Wang 2011).

3.1 CPK-based security authentication technology

The CPK-based security authentication technology is used to implement identity authentication between nodes and protocol interaction so as to ensure the integrity and authenticity of data transmission (Chang and Chen 2012; Rauter et al. 2016). The working principle is as follows: Initially, the data packets are securely hashed, and the private key of the current node ID is operated by the signature operation, the signature data is obtained. Thus, the data packet is sent to the opposite end; the receiving end verifies its legitimacy according to the data packet carried in the node ID. In addition, in order to prevent information leakage, symmetric key encryption technology is adopted to implement secure transmission and reception of protocols between nodes; CPK technology is used to implement negotiation of session keys between nodes. The process of information exchange based on CPK is shown in related work. The key negotiation can be completed only with one interaction. It is not necessary to transfer the session key in the network, which ensures the security of key transfer (Gong et al. 2017, 2018; Wang and Liu 2018).

Compared with traditional public key infrastructure (PKI), digital signatures, and other technologies, CPK-based security authentication technology does not require third-party certification and online database support, a single chip can be achieved, and has the advantages of economy, high efficiency, and large-scale support in engineering applications. Therefore, it can effectively compensate for the shortcomings of security authentication mechanism that is simple and can be easily cracked in Open Shortest Path First (Open_SPF) (Ma et al. 2017; Ziegeldorf et al. 2013).

3.2 Trusted delivery

In order to achieve the SLSRP, a trusted transformation is done without damaging the integrity of Open_SPF. The length of the ***Authentication*** field in the Open_SPF protocol common packet header is extended from 64 to 128 bits so as to store the CPK signature. In addition, LINK TLV packets in Open_SPF are populated with node trusted measurement information.

Before the trusted transmission in the SLSRP protocol, the current node firstly uses the Trusted Measurement Model based on Dynamic Bayesian Networks to complete the trusted calculation of the neighborhood node and form a local trusted relationship list. Then, in the process of the protocol interaction such as neighbor discovery and link state flooding, the CPK-based security authentication mechanism is adopted to ensure that the identity of the protocol interaction peers is trusted, and the carried trusted information is securely transmitted and diffused across the entire network to form a unified link state database that contains trusted information across the entire network. Finally, the Constrained Shortest Path First (CSPF) algorithm is used to calculate the optimal path that satisfies the trusted measurement requirement. The trusted transfer control process of the Secure link state routing protocol is shown in Fig. 3.

3.3 Trusted routing computation

Definition 2 Let $v_s, v_d \in V$, $v_s \neq v_d$ denotes the source and destination nodes, respectively. If each node that constitutes a trusted path can meet the confidentiality, availability, and integrity requirements in process of information transmission and can provide predictable security and trusted services, then $P(v_s, v_d) = \{v_s, \ldots, v_d\}$ is called as a trusted path between node v_s and v_d in network G.

The cost of the trusted path is represented by C and its expression is written as follows:

$$C(v_s, v_d, D) = \sum_{i=s}^{d} (1/T_i) \tag{6}$$

where $T \in [0, 1]$ is a constant; C is the cost of the trusted path between node v_s and v_d under the constraint condition that the node's trusted measurement is T; $C \in [0, \max]$, and max is the upper limit value of the system hypothesis.

In the routing calculation, SLSRP selects the smallest C as path on the basis of the node's comprehensive trusted measurement. When only one path between node v_s and v_d satisfies the required trusted path, the path is the optimal path; when there are multiple trusted paths that satisfy the requirement, there must be a comprehensive consideration of the length of the trusted path, and the trusted measurement jitter.

The average of the trusted measurement in the trusted path is denoted as M and its expression is

$$M_x = (1/L(P_x)) \sum_{i=s}^{d} T_i \tag{7}$$

where P_x, M_x denote the x-th trusted path and its node trusted measurement average, respectively; P_x indicates the length of the x-th trusted path.

The trusted measurement jitter of the trusted path is denoted as V, and its expression is

$$V_x = (1/L(P_x)) \sum_{i=s}^{d} (T_i - M_x)^2 \tag{8}$$

where V_x denotes the trusted measurement jitter of the x-th trusted path.

The calculation process of the Optimization Trusted Path First (OTPF) of the secure link state routing protocol is shown as follows.

Input: V_s, V_d, G

Output: P_{best}

Begin

(1) $P_{\min Len} = \Phi, P_{best} = \Phi, \ P_{best\_V} = \Phi$

(2) $\mathrm{P} = tDijkstra(G, V_s, V_d)$

If$(P! = \Phi)$

(3) If(P.GetSize() > 1)

$P_{\min Len} = \mathrm{Length\_first\_Cal}(P)$

(4) If($\mathrm{P}_{\mathrm{minLen}}$.GetSize() > 1)

$P_{\mathrm{best\_V}} = \mathrm{V\_first\_Cal}(P_{\min Len})$

End if

(5) If($\mathrm{P}_{\mathrm{best\_V}}$.GetSize() > 1)

$P_{best} = \mathrm{M\_first\_Cal}(P)$

End if

Else

$P_{best} = P$

Else

$P_{best} = \Phi$ End if

End

Step (2) calculates the node trusted path set P in the network G according to the improved shortest path *Dijkstra* algorithm ; If there are multiple trusted paths that meet the requirements in step (3), select the path with the shortest path length according to the shortest path first principle; if there are multiple shortest trusted paths with the same length in step (4), then the trusted path with the smallest jitter is selected on basis of the least priority principle of trusted measurement jitte. In step (5), if there are multiple shortest trusted paths with the same jitter, the trusted path with the largest average value is selected according to the maximum priority principle of trusted measurement.

4 Simulation experiment and analysis

In order to verify our proposed trusted measurement model based on dynamic Bayesian networks, we design some experiments to test its performance. The simulations are all implemented by MATLAB (R2010a) on a personal computer with 4-GB memory, 2.94-GHz Intel Core i5-7500 processor. The simulation experiment mainly validates and analyzes the effectiveness of the secure link state routing protocol.

4.1 Parameter configuration

In experiment, the OPNET Modeler network is used as simulation platform, where the secure link state routing protocol is simulated and modeled. The simulation scenario consists of 38 core routers, 2 access routers, and 2 user nodes. All core routers form the core routing domain. Services are generated by *Src* node and arrive to *Dest* node after crossing the network. Parameter settings are shown in Table 1.

4.2 Simulation and analysis

According to the experimental setup, the simulation experiment is conducted. Through the comparison of SLSRP and Open_SPF in the same scenario, the timeliness and dynamic self-adaptability of SLSRP are analyzed and verified.

Firstly, the SLSRP and Open_SPF protocol overheads are compared. The real-time protocol overhead is shown in Fig. 2. The average protocol overhead is shown in Fig. 3. The red-connected curve is SLSRP and the green connection curve is Open_SPF. At the beginning of the simulation, the route jitter caused the protocol overhead of the secure link state routing protocol and Open_SPF to be large, reaching the peak around 36 s.

In addition, the protocol overhead of our proposed algorithm is increased by about 57% compared with Open_SPF, and then both our algorithm and Open_SPF complete the route convergence in 80 s. and the protocol overhead is not significantly different. As a whole, the average protocol overhead for our improved algorithm is approximately 11.7% higher than that of Open_SPF, which is mainly caused by the authentication mechanism introduced by SLSRP; after a denial of service attack at 500, 700, and 900 s in simulation time, the change of the reliability causes the secure link state routing protocol to trigger the route calculation again. Therefore, the protocol overhead of the improved algorithm is significantly larger than that of Open_SPF. At other times, the two protocol overheads are not much different.

After 500, 700, and 900 s at the simulation time, the network is subjected to a denial of service attack, which causes the secure link state routing protocol triggers route calculation again because of the change of the node's reliability. Therefore, the protocol overhead of SLSRP is significantly larger than that of Open_SPF, and there is little difference in the protocol overhead at other time.

Comparing the end-to-end time delay of the secure link state routing protocol with that of Open_SPF, the result is shown in Fig. 4, where the blue curve represents the Open_SPF when the number of attack nodes is 0, and the red and green curves represent the results when the number of attacked nodes is 0 and 3. Due to the additional cost of CPK mechanism, the delay of our proposed algorithm is slightly larger when the number of attacked nodes is 0. Since Open_SPF cannot obtain the change of the link state in time when nodes LSR20/17/2 are subjected to denial of service attacks at simulation time 500, 700,

Table 1 Parameter settings

Parameter/event	Description
Simulation time (s)	1800
Penalty factor	0.5
Attenuation factor	0.1
Simulation event 1	100 s, generate specific business
Simulation event 2	500 s, denial of service attack
Simulation event 3	700 s, randomly launch denial of service attacks
Simulation event 4	900 s, randomly launched denial of service attacks
Simulation event 5	1100 s, stop the attack
Business features	20 packets/s, 80 bit/packet
Downtime interval (s)	54

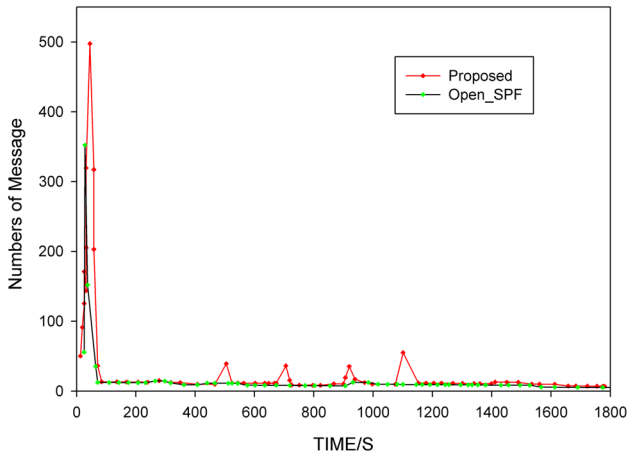

Fig. 2 Comparison for real-time protocol overhead

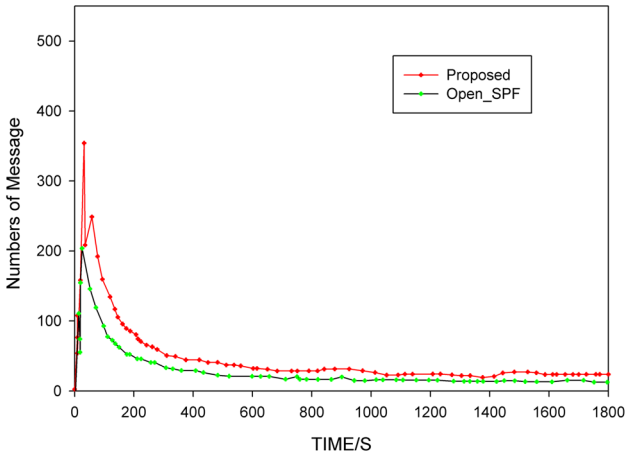

Fig. 3 Comparison for average protocol overhead

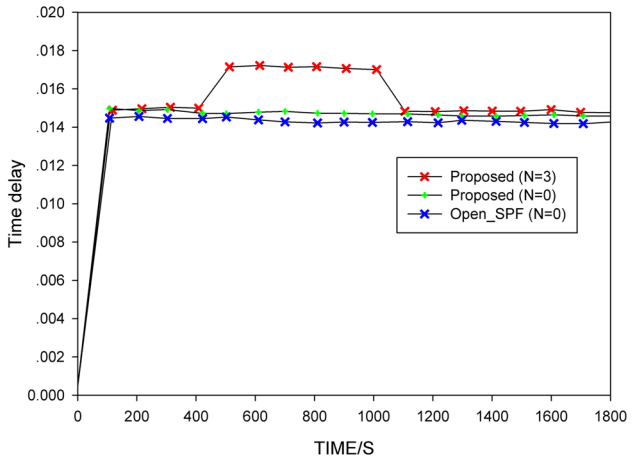

Fig. 4 Comparison for end-to-end time delay

and 900 s, respectively the route recalculation is triggered after the timeout interval of 54 s, which causes a significant increase in delay. Therefore, Open_SPF protocol is difficult to quickly respond to denial of service attack. Under the same condition, our algorithm can get the change of the node trusted measurement in time and trigger the routing recalculation. In addition, the re-convergence of the route only adds a small time overhead.

During the whole simulation process, our proposed algorithm is completed by the trusted measurement module embedded in the device model, which only slightly increases the computational complexity of the node model under the unrestricted resource condition, and has little influence on the complexity and overhead of the network system. With the changes of the network state and subsequent attacks, the selection of the optimal trusted path has changed for four times.

Experimental results show that our proposed algorithm can complete route convergence and service forwarding under normal conditions, which proves its effectiveness. Compared with Open_SPF, our algorithm has almost the same route convergence and service transmission time, but the protocol overhead is slightly greater; when the network suffers a denial of service attack, the trust and authentication mechanism introduced by our algorithm does not significantly increase the protocol overhead and complexity compared with Open_SPF. At the same time, it can obtain the change of node trusted measurement in time and trigger route calculation again, so our algorithm has a better dynamic adaptive ability and timeliness, and can choose a high security and reliable path for information transmission, effectively resisting denial of service attacks.

5 Conclusion

Aiming at the insecure network environment, a secure link state routing protocol based on the node trusted measurement is proposed in this paper. Through the introduction of a trusted mechanism in the network, our algorithm considers the node trusted measurement and path trusted measurement during route calculation in an integrated manner, and the CPK-based security authentication technology is adopted to enhance the security of the protocol interaction. Simulation experiments show that our algorithm has a better timeliness and dynamic adaptive ability in the case of a denial of service attack, which lays a good foundation for the trusted network connection technology. The future work is to optimize our algorithm and further study the routing jitter problem of the secure link state routing protocol under continuous attack.

References

Ammireddy A (2017) Method and system for efficient graceful restart in an open shortest path first (Open_SPF) network

Aris A, Oktug SF, Yalcin SBO (2015) Internet-of-Things security: denial of service attacks, pp 903–906

Bamasag O, Toumi KY (2016) Efficient multicast authentication in Internet of Things. In: International conference on information and communication technology convergence. IEEE, Piscataway, pp 429–435

Chang KD, Chen JL (2012) A survey of trust management in WSNS, Internet of Things and future Internet. KSII Trans Internet Inf Syst 6(1):5–23

Gang G, Lu Z, Jiang J (2011) Internet of Things security analysis. In: International conference on internet technology and applications. IEEE, Piscataway, pp 1–4

Gong B, Zhang Y, Wang Y (2017) A remote attestation mechanism for the sensing layer nodes of the Internet of Things. Future Gener Comput Syst 78:867–886

Gong B, Wang Y, Liu X et al (2018) A trusted attestation mechanism for the sensing nodes of Internet of Things based on dynamic trusted measurement. China Commun 15(2):100–121

Griffin PH (1992) Security for ambient assisted living: multi-factor authentication in the Internet of Things. In: IEEE GLOBECOM workshops. IEEE, Piscataway, pp 1–5

Kothmayr T, Schmitt C, Hu W et al (2013) DTLS based security and two-way authentication for the Internet of Things. Ad Hoc Netw 11(8):2710–2723

Ma Z, Wang Z, Liang D et al (2017) A model of trusted measurement model, p 04023

Ndibanje B, Lee HJ, Lee SG (2014) Security analysis and improvements of authentication and access control in the Internet of Things. Sensors 14(8):14786–14805

Park N, Kang N (2015) Mutual authentication scheme in secure Internet of Things technology for comfortable lifestyle. Sensors 16(1):20

Rauter T, Iber J, Kreiner C (2016) Thingtegrity: a scalable trusted computing architecture for the Internet of Things. In: International conference on embedded wireless systems and networks. Junction Publishing, Toronto, pp 23–34

Sun X, Wang C (2011) The research of security technology in the Internet of Things. In: Advances in computer science, intelligent system and environment. DBLP, pp 113–119

Sun K, Quan LI, Xiaofeng XU et al (2017) Risk analysis on human factors in operation of high risk construction based on dynamic Bayesian network. J Hydroelectr Eng 36(5):28–35

Tamboli MB, Dambawade D (2017) Secure and efficient CoAP based authentication and access control for Internet of Things (IoT). In: IEEE international conference on recent trends in electronics, information and communication technology. IEEE, Piscataway, pp 1245–1250

Teng M, Li B, Zhai N (2017) Study on data security protection technology in Internet of Things. China Comput Commun

Wang L, Liu F (2018) A trusted measurement model based on dynamic policy and privacy protection in IaaS security domain. EURASIP J Inf Secur 2018(1):1

Wang L, Jiang S, Guo Y (2012) Composable-secure authentication protocol for mobile sensors roaming in the Internet of Things. Sci Sin 42(7):815

Wang J, Fan K, Mo W et al (2016) A method for information security risk assessment based on the dynamic Bayesian network. In: International conference on networking and network applications. IEEE, Piscataway, pp 279–283

Wu F, Xu L, Kumari S et al (2017) A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security. J Ambient Intell Humaniz Comput 8(1):101–116

Xiao Q, Liu S (2017) Motion retrieval based on dynamic bayesian network and canonical time warping. Soft Comput 2:1–14

Zhang Q, Feng D, Zhao S (2016) Research of platform identity attestation based on trusted chip. J Commun 35(8):95–106

Zhao YL (2013) Research on data security technology in Internet of Things. Appl Mech Mater 433–435:1752–1755

Ziegeldorf JH, Shafagh H, Raza S et al (2013) Towards viable certificate-based authentication for the internet of things. In: ACM workshop on hot topics on wireless network security and privacy. ACM, New York, pp 37–42