An Identity Authentication Scheme Based on Node Behaviors for Wireless Sensor Networks

Guanghui Chang[1, a], Shaofei Liang[2, b] and Guangxia Xu[3, 1, c]

[1] School of Software Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

[2] School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

[3] The Information and Communication Engineering Postdoctoral Research Station, Chongqing University, Chongqing 400044, China

[a]Changgh@cqupt.edu.cn, [b]s130101094@stu.cqupt.edu.cn, [c]xugx@cqupt.edu.cn

Keywords: identity authentication, behaviors of node, trust mechanism, insider attack.

Abstract. Identity authentication is a crucial security issue in wireless sensor networks, because wireless sensor nodes are typically deployed in an unattended environment, leaving them open to possible hostile network attacks. We propose a new identity authentication scheme based on the behaviors of node in wireless sensor networks. Our scheme which depends on trust mechanism can resist the insider attacks effectively. With the total trust value integrated with direct trust value, recommendation trust value and history trust value of nodes, we can verify identity of nodes. Experiments indicate that our scheme is ideal to enhance the solution for identity authentication of nodes. Moreover, it can against the insider attacks effectively.

Introduction

Wireless sensor networks (WSNs) are rapidly becoming a significant part of Internet of things[1]. And the data which are collected by the wireless sensor nodes are related closely to our privacy and some other security issues[2]. Due to the open environment of WSNs, wireless sensor nodes will be usually faced with many threats including capture, compromise, denial of service attacks and replay attack etc. which will damage the privacy of data and do harm to the whole network directly. It is important to protect the data and the nodes themselves especially for that they are easily attacked without identity authentication. The ordinary methods of identity authentication which goal is to make sure the legal identity of nodes and to build up a truth relationship of each legal node are mostly based on the technology of encryption[3].However, these methods are too complex and slow to meet the need of WSNs which are resource-constrained. And the applications of WSNs are with the features that make it hard for researchers to enhance the identity authentication. (1) WSNs are large-scale, resource-constrained and with a weak compute capability, (2) the open environment of WSNs make nodes easily attacked by stealing attack, (3) the nodes have a poor ability to against the insider attacks.

Related Work about Authentication

In 2006, a simpler dynamic user authentication protocol based on exclusive-or operations and one-way hash functions in WSNs[4] was put forward. The protocol imposes very light computational load and requires simple operations. However, this protocol requests that users query sensor nodes in a specific limited time for a certain purpose. And for the predefined time limit, users have to re-register itself according to the future requirements. A two-factor user authentication protocol[5] which provided strong authentication and a session of key establishment for WSNs existed in 2009, this authentication means that more than one factor is required to authenticate the communicating party in the authentication mechanism. B. Vaidya et al.[6] improved the two factor authentication

scheme, because it is vulnerable to stolen smart card attacks and it did not provide a key agreement. J. Kim et al.[7] presented that gateway node bypassing attacks and user impersonation attacks are possible using secret data stored in a sensor or an attacker's own smart card in Vaidya et al.'s scheme. Besides they proposed scheme resisted user impersonation attacks and gateway node bypassing attacks using secret data stored in an attacker's own smart card or a sensor. J.H. Guo et al.[8] proposed DDA-MBAS which is a multi-user broadcast authentication scheme in wireless sensor networks with defending against DoS attacks. Their scheme which is based on vBNN-IBS signature and hash operation can not only defends against node compromise attack but also costs less energy. P. Mahalakshmi et al.[9] proposed an authentication method based on a compromised node detection protocol. And a novel and efficient source anonymous message authentication scheme (SAMA) based on elliptic curve cryptography (ECC) was used.

Distributed authentication is suit for WSNs which are large-scale, resource-constrained and with a weak capability. A novel distributed authentication scheme (NDAS[10])which was based on the well-known concept of "secret sharing" cryptography and group "consensus" was proposed. D. He et al.[11] proposed an application-independent and distributed trust evaluation model for MSNs, simple cryptographic techniques were used. V. Geetha et al.[12] designed a trust management system for WSNs which is based on parameters and trust factors. Recently, an Efficient Distributed Trust Model (EDTM[13]) for WSNs was proposed. Instead of only taking communication behavior into account, EDTM introduced direct trust and recommendation trust based on communication behavior.

Proposed Scheme

Network Model

In order to make our scheme clear we made the following assumptions: Nodes are legal at the beginning of deployment and they have the same trust values; The sensor nodes are stationary after deployed and the moving nodes are not considered in this paper; And there are three kinds of nodes in the networks: wireless sensor node which collects information directly; cluster nodes which collects information from wireless sensor nodes within their communication scope; base station which deals with the information collected by cluster nodes and communication with other networks, is credible all the time.

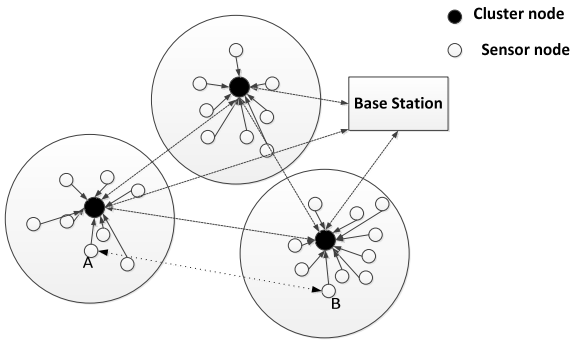


Fig.1 Network Model

Fig.1 shows the sensor network model. Nodes of networks can't communicate with each other directly. When node A wants to communicate with node B, it has to send a message to the its cluster and the cluster then to send the message to the cluster of node B, and node B has to go the same way to communicate with node A. Clusters in the networks can not only communicate with each other within their communication scope but also communicate with the base station.

Authentication Mechanism

The direct trust value of authenticated node will be figured out by the cluster of it according to the transmission delay and packet loss rate. And the recommendation trust value will be figure out when the cluster of authenticate node has received the recommendation trust values of each cluster nodes which are the neighbor of authenticated node. At last combined with direct trust T_d recommendation trust T_r and history trust T_h which are stored by the cluster of authenticate node then the total trust

value T_t of authenticated node will got. Comparing the total trust value T_t of authenticated node with the threshold trust value $T_{\min}$, When $T_t \geq T_{\min}$ the node authenticated will be considered as a legal member, the authenticated node can exchange information with other nodes among the network and store T_t for next time authentication. Otherwise, $T_t < T_{\min}$ the node will be considered as illegal one, thus it will be isolated from the network. The process of authentication is shown in Fig.2.

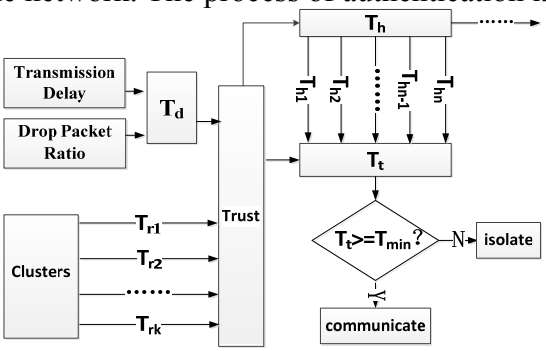


Fig.2 Overview of Authentication

Direct Trust: To assume the range of normal transmission delay is $[\alpha_1, \alpha_2]$, when the transmission delay of node is out of the range, it will be considered as abnormal delay, and the node with abnormal delay may be considered as compromised or it is broken. The farther the actual transmission delay of nodes deviates from the normal range, the more likely that the node is compromised and the higher possibility that it will attack the networks. The evaluation method of transmission delay is:

$$T_{delay} = \begin{cases} c^{\beta} & if \quad D \notin [\alpha_1, \alpha_2] \\ 1 & else \quad D \in [\alpha_1, \alpha_2] \end{cases}. \tag{1}$$

Where D is transmission delay, β is the interval offset, and $c < 1$, when D is within the range $[\alpha_1, \alpha_2]$ the T_{delay} equals 1, the node will be considered as a legal one.

According to Beta Distribution Model[14], we set the trust value $\frac{M+1}{N+2}$ on authenticated nodes, which means that authenticated nodes are requested to forward N packets and M of them are forwarded successfully, $N \geq M$. The evaluation of behaviors of packet loss rate will be as Equation 2:

$$T_{loss} = \log_2(1 + \frac{M+1}{N+2}). \tag{2}$$

The direct trust value is described as Equation 3:

$$T_{direct} = \lambda T_{loss} + \mu T_{delay}. \tag{3}$$

Where $0 < \lambda < 1, 0 < \mu < 1$, and $\lambda + \mu = 1$. Values of λ and μ will be determined according to the specific network environment.

Recommendation Trust: In order to make the recommendation trust more reasonable and fair more than one cluster nodes which are neighbors of authenticated nodes should be asked for the recommendation trust. And then compare each trust value sent by different clusters with mean value of multiple recommendation trust value and figure out the offset of them. They are shown as Equation 4 and Equation 5 below:

$$E(\mathrm{r}) = \frac{1}{k}\sum_{i=1}^{k} r_i. \tag{4}$$

$$\sigma = \sum_{i=1}^{k} \frac{|r_i - E(r)|}{k}. \tag{5}$$

Where k is the number of recommendation trust value and it will be determined according to the specific network environment， r_i is the recommendation trust value of clusters.

According to Equation 4 and Equation 5, the new recommendation trust value for this paper will be defined as Equation 6:

$$T_{recommendation} = \log_2(2-\sigma). \tag{6}$$

And it can proofed that the scope of σ is $[0,1]$, so the scope of $T_{recommendation}$ will be $[0,1]$.The value of $T_{recommendation}$ will decrease as the value of σ raises, which means the value of $T_{recommendation}$ depends on σ.

History Trust: Two sensor nodes had communicated with each other for $(\upsilon+\omega)$ times and the number of normal communication is υ and the abnormal one is ω, then we define that history trust value as below:

$$T_{history} = \frac{\upsilon+1}{\upsilon+\omega+2}. \tag{7}$$

Total Trust: The main task of modelling the behaviors of node is to make a comprehensive evaluation of behaviors of node. Total trust is related to T_{direct}, $T_{recommendation}$ and $T_{history}$ so the weighting coefficient W_i must be required.

$$T_{total} = \left[W_1 \times T_{direct} + W_2 \times T_{recommendation} + W_3 \times T_{history}\right]. \tag{8}$$

Total trust value T_{total} depends more on T_{direct} than $T_{recommendation}$ and $T_{history}$. $0 \le W_3 < W_2 \le W_1 \le 1$, $W_1 + W_2 + W_3 = 1$, W_i is determined according to the specific network environment.

Algorithm 1 Trust based authentication algorithm

Input: T_{direct}, $T_{recommendation}$, $T_{history}$, trust queue Q, trust threshold $T_{\min}$

Output: The flag for that authenticated node becomes an illegal node

//initiation

1: **if** $Q = \varnothing$

2: Initial all records with uncertain trust and put them into Q.

3: **end if**

//collection

4: Collect recommendation trust values

5: Authenticate node Calculates total trust T_{total} for authenticated node and inserts it to the rear of Q.

//authentication

6: **if** $T_{total} < T_{\min}$

7: **return** false

8: **else**

9: **if** $T_{total} \ge T_{\min}$

10: **return** true

11: **end if**

12: **end else**

13: **end if**

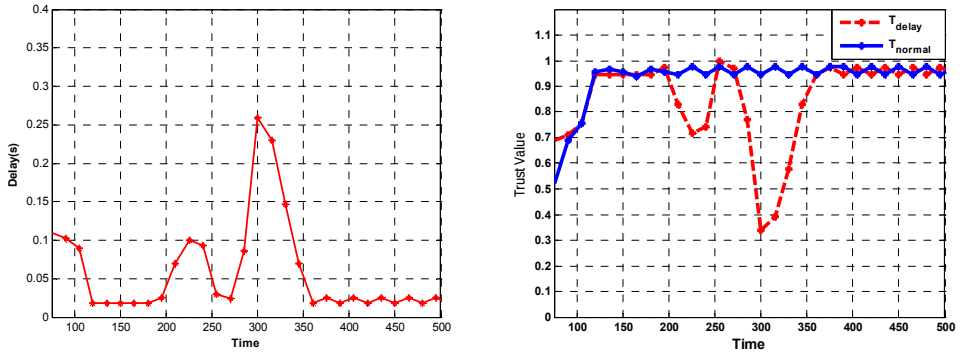
The input of this algorithm are T_{direct}, $T_{recommendation}$, $T_{history}$ and the trust threshold $T_{\min}$. The initiation phase costs $T_{init} = O(n)$,for that the length of queue which will be used to store the history trust value

is n; Besides, in the phase of collection r recommendation trust value will be collected, collecting recommendation trust values costs $T_{collect} = O(r)$; The authentication phase costs $T_{autheticate} = O(1)$. Based on the analysis above, the total time complexity of the algorithm is $T = T_{init} + T_{collect} + T_{authenticate} \sim O(n+r)$.

Simulation and Analysis

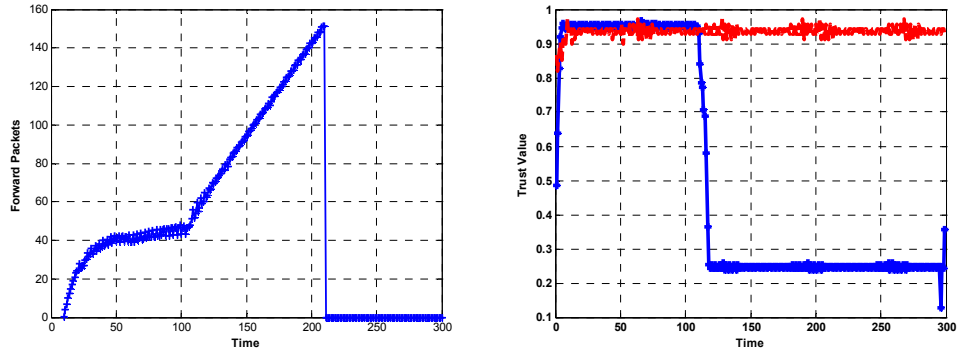
There will be two types of illegal nodes in our simulations: the node with longer transmission delay and the other with higher packet loss rate. Our simulations will add the two types of nodes in respectively to check whether the proposed scheme will discover the illegal nodes and isolate them in time.

We show an attack which the node with transmission delay longer than legitimate nodes and its change of trust value. Fig.3(a) shows us the attack begins and stops at the system time 270 and 335, respectively. The results for the individual attack type are plotted in Fig.3(b).It is clear that the trust value of a legitimate node(The blue one) increases rapidly(They have the same trust value which is 0.5 at the beginning of simulation), becoming more than 0.94 after a short time and remaining stable. During the system time 270 to 335 the trust value of the malicious node (The red one) decreases rapidly, becoming less than 0.4 after a short time because transmission delay of it seriously deviates from the normal range during that system time. Besides, once a malicious node finishes attacking (e.g., the node has been replaced), the dynamics of its trust value exhibits similar behaviors as that of legitimate node. Our scheme is work to identify the nodes which have compromised in time.



(a) Transmission delay (b) Trust value of delay node

Fig.3 Transmission delay and the corresponding trust value of node



(a)Forward Packet (b) Trust Value

Fig.4 Trust Value of Lose Node

Attacks caused by denial of service (DoS) is called DoS attack, which is to make the node or network out of work, such as resulting in large packet loss rate or low packet forwarding rate. When the number of forwarding packets increases over the capacity of the node, DoS fault occurs. As shown in Fig.4(a), the forwarding packets of node is increasing between the system time 100 and 210, which is to make the node result in DoS fault. Fig.4(b) is the corresponding trust value curve of the

node. At system time 110 When DoS fault of node occurs trust value of node drops to 0.25(The blue one). The above results demonstrate that the proposed scheme can effectively identify abnormal behavior of the authentication nodes when DoS fault occurs.

Fig.5 demonstrates the different communication overhead E_c of networks with different number of recommendation nodes N_r and different number of wireless sensor nodes N in the networks. It can conclude that when N_r is certain the relationship of E_c and N is proportional, the larger N is the higher E_c will be requested. And when N is certain, the relationship of E_c and N_r is proportional. E_c will rise when N_r is increased. Therefore, we should minimize N_r under the premise that network can hold a high correct rate in judging the behaviors of nodes.

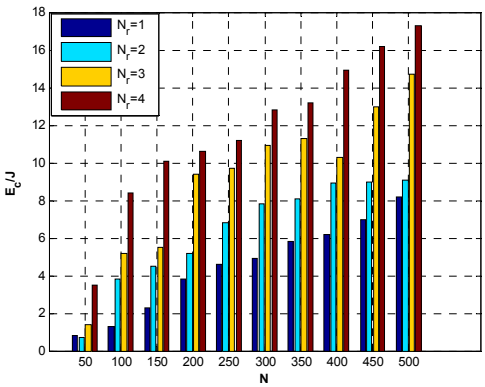


Fig.5 Communication Overhead of Different Number of Recommendation Node

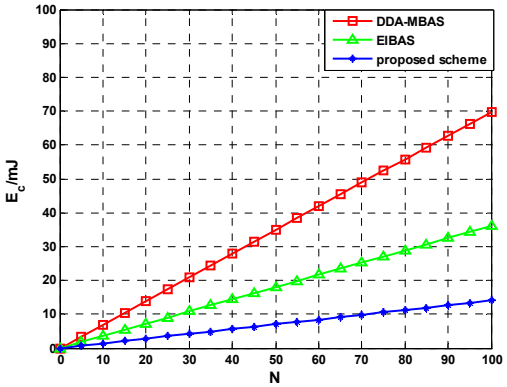


Fig.6 Communication Overhead of Different schemes

We compare our proposed scheme with the DDA-MBAS[8] and EIBAS[15] which are authentication schemes based on though of broadcast communication in theory. We compare them on communication overhead. As showed in Fig.6 three schemes will cost more energy in WSNs when the number of their neighbors raise, because while authenticating a new node in or out of the networks they have to communicate with their neighbors, as a result they have to cost energy to send or receive message. Besides, DDA-MBAS costs the most energy, EIBAS costs the second most energy during the process of authentication, and our proposed scheme cost the less energy. The reason of that phenomenon is the difference of the message length they needed to exchange during the process.

Conclusion

An identity authentication scheme for WSNs based on node behavior is proposed and that scheme is proved to have a good effect on preventing the nodes from insider attacks due to the node compromise. Our scheme can effective identify the compromise nodes, because we authenticate node's identity not only rely on their behaviors but also rely on the recommendation trust value of their neighbor clusters. The communication overhead of our scheme is lower than some other scheme which based on broadcast communication, because without the process of authenticated node

communicates with their neighbor clusters. And the communication overhead will rise with the number of recommendation trust in the network.

Acknowledgment

The authors acknowledge support from the Project Foundation of Chongqing Municipal Education Committee (No. KJ1500441), the National Natural Science Foundation (No. 61309032, No. 61272400), China Postdoctoral Fund (No. 2014M562282), the Project Postdoctoral Supported in Chongqing (No. Xm2014039), Collaborative Innovation Center for Information Communication Technology (No. 002), the Comprehensive Technology Application Demonstrated Project of Safety Smart City in Nan'an District of Chongqing city (No. 2013GS500303-Y3), Research on Intelligent Big Data Analysis and Process Technology for Business Intelligent (No. A2015-44).

References

[1] S. Li, L.D. Xu, and S. Zhao. "The internet of things: a survey." Information Systems Frontiers, vol.17.2 (2015), p.243-259.

[2] R.H. Weber, "Internet of Things-New security and privacy challenges," Computer Law & Security Review, vol.26 (2010), p.23-30.

[3] Y. Zhou, Y. Fang and Y. Zhang, "Security wireless sensor networks: a survey," IEEE Communication surveys and tutorials, vol. 10 (2008), pp. 6-28.

[4] K. Wong, Y. Zheng, J. Cao and S. Wang, "A Dynamic User Authentication Scheme for Wireless Sensor Networks," in: Proc. IEEE International Conf. Sensor Networks, Ubiquitous, Trustworthy Computing, IEEE Computer Society, 2006, p. 244-251.

[5] M.L. Das, "Two-factor user authentication in wireless sensor networks," Wireless Communications, IEEE Transactions on, vol. 8(2009), p.1086-1090.

[6] B. Vaidya, M. Dimitrios and M. Hussein, "Two-factor mutual authentication with key agreement in wireless sensor networks," Security and Communication Networks, 2012.

[7] J. Kim, D. Lee, W. Jeon, Y. Lee and D. Won "Security analysis and improvements of two-factor mutual authentication with key agreement in wireless sensor networks," Sensors, vol.14.4 (2014), p.6443-6462.

[8] J.H. Guo, M.A. Jian-Feng. "Multi-user broadcast authentication scheme in wireless sensor networks with defending against DoS attacks." Journal on Communications, vol.32 (2011), p.94-102.

[9] P. Mahalakshmi and G.P. Babu, "Compromised Node Identification for Message Authentication in WSNs," International Journal, vol.3.6 (2015).

[10] K. Bauer, L. Hyunyoung, "A distributed authentication scheme for a wireless sensing system," ACM Transactions on Information and System Security, vol.11 (2008), p.1-35.

[11] D. He, C. Chun, C. Sammy, J. Bu and Vasilakos, "A Distributed Trust Evaluation Model and Its Application Scenarios for Medical Sensor Networks." Information Technology in Biomedicine IEEE Transactions on, vol.16 (2012), p.1164-1175.

[12] V. Geetha, K. Chandrasekaran. "A Distributed Trust Based Secure Communication Framework for Wireless Sensor Network." Wireless Sensor Network, vol.06 (2014).

[13] J. Jiang, G. Han, F. Wang, L. Shu and M. Guizani, "An efficient distributed trust model for wireless sensor networks," Parallel and Distributed Systems, IEEE Transactions on, vol.26.5 (2015), p.1228-1237.

[14] I. Jøsang, Roslan and B. Colin, "A survey of trust and reputation systems for online service provision," Decision Support Systems, vol. 43 (2007), p. 618 - 644.

[15] K.A. Shim, Y.R. Lee and C.M. Park. "EIBAS: An efficient identity-based broadcast authentication scheme in wireless sensor networks." Ad Hoc Networks, vol.11 (2013), p.182-189.