Trust Based Authentication Mechanism in Wireless Sensor Networks

http://dx.doi.org/10.3991/ijoe.v12i01.5173

Ru-ping Li
Anhui Business Vocational College, Hefei City, Anhui Province, China

***Abstract*—Authentication mechanism is the basis of access control and data exchange. In wireless sensor networks, the vulnerability of network nodes and complexity of communication protocols pose a huge challenge for designing authentication mechanism in such environment. In this paper, we study the authentication mechanism in wireless sensor networks based on trust between nodes. We use the interaction history of nodes for recommendation trust computation, and the interaction history comes from the interactions between nodes. We design a penalty mechanism for hostile nodes based on the TCP congestion control protocol, and present a loyalty based trust recommendation evaluation algorithm. Massive experiments validate the efficiency and effectiveness of the proposed approach.**

***Index Terms*—wireless sensor networks; authentication; trust; network security**

I. INTRODUCTION

Wireless sensor networks are the combination of computing, communication and sensors, and they can be used to acquire and process data in an absolutely new way [1]. Nowadays, Wireless sensor networks have been extensively deployed in environment monitoring [2] healthcare [3], industrial control [4], military field [5], and so on. With the rapid development of sensors and related techniques, wireless sensor networks are more and more ubiquitous. Just like Internet on the Web, people and their environment will eventually be an Internet of things [6]. However in many applications, people have very high demand for security in wireless sensor networks. In order to keep the effectiveness and confidentiality of applications, security is one of the most important issues in deploying wireless sensor networks [1, 7].

Authentication is the most important issue in network security, and it includes entity authentication [8] and message authentication [9]. Entity authentication is the primary problem in access control, and it is the first barrier of security in wireless sensor networks. According to definition of cryptography, entity authentication is the identity authentication process from one user to another, and it provides secure access mechanism for network access. Message authentication mainly aims to confirm the validity of data source and keep the integrity of data, and it prevents non-authentication users from sending, fabricating and tampering data. Because of the limits of computation, storage and energy [10], traditional authentication mechanisms of networks cannot be used in wireless sensor networks directly.

In this paper, we study the authentication mechanism of wireless sensor networks based on trust between objects. We use the interaction history of objects for recommendation trust computation, and apply the slide window technique to capture the interactions between objects. The rest of the paper is organized as follows. In section 2, we review related works about authentication mechanism in network and information access. In section 3, we present our proposed trust based authentication mechanism. Experiments and conclusion are given in section 4 and 5 respectively.

II. RELATED WORKS

Traditional authentication methods include user-name & password, personal identification number (PIN), text, sudoku, and so on. When authenticating with the above methods, the input passwords can be easily stole. In addition, simple passwords can also be cracked easily, and complex passwords are hard to memorize. So, much more easy-to-use and reliable authentication mechanisms are needed [11].

Biometrics identification technologies [12] are good complements for traditional identity authentication mechanisms. Biometrics based authentication is secure, reliable and convenient, and has attracted more and more attention from both academic and industry. Biometrics authentication technologies, such as face authentication [13], fingerprint authentication [14], iris authentication [15], handwriting authentication [16], etc., have developed rapidly in the last decade. However for authentication on handhold devices, the above biometrics based technologies need special hardware, and thus the prices are very high.

With the explosive increase of smart phones on the market, more and more smart phones integrate with many sensors, e.g. accelerometer and gyroscope. These sensors can be combined with software on the smart phones to sense human behaviours cheaply and efficiently, and thus can be used to identify people's biometrics. The newly generated authentication technologies on smart phones include tri-axis accelerometer based gait authentication [17, 18], correlating trajectory and password based authentication [19, 20], and so on.

Based on the idea of gait recognition, Farella et al. [21] analyze the biology features of human and collect gait features from accelerometer sensor. According to dimension reduction and classification of sensed data, they propose gait features based authentication approach, and the approach is used for authentication in a small group of people. Liu et al. [22] apply the method proposed in [21] in the non-imitating-attacking situation, and get a good result, so the prospect of authentication based on collecting sensed data and recognizing gait features is optimistic. In addition, researches [23, 24, 25] describe several au-

thentication approaches based on gait recognition via tri-axis accelerometer. Okumura et al. [23] authenticate via some fixed gait, but their method doesn't support user-defined gait. In order to acquire equal error rate, the method proposed in [24] needs more training samples. The focus of [25] is mainly on the accuracy of gait recognition in human-computer interaction, however in the imitating-attacking situation, the equal error rate is still about 10%, so it can't be used to authenticate on critical information.

In addition, practicability and real-time capability are two main requirements of authentication on mobile devices. They must satisfy less required training samples and shorter time of authentication [26], and must be unaffected by surrounding environment. So, the methods based on statistical machine learning, visual features, speech recognition etc., have their own limits.

III. TRUST BASED AUTHENTICATION MECHANISM

In this section, we propose a trust based authentication mechanism, and it is depicted in figure 1.

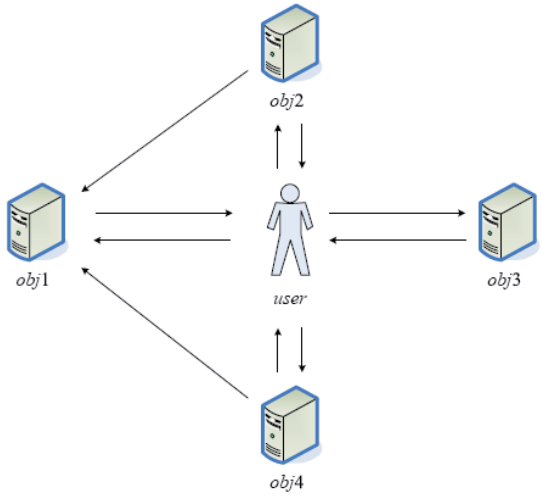

Figure 1. Structure of authentication mechanism

In figure 1, each object is denoted as a sensor node, the links between the user and objects are directed. And each directed link is a trust action. For example, $TRUST(A,B)$ means user (or object) A trusts object (or user) B, and the value is $0 \le TRUST(A,B) \le 1$. Moreover, the links between objects are also directed, and each link presents a recommendation action. For example, $RECOM(obj1,obj2)$ means $obj1$ has recommended $obj2$ to the user, and the value of $RECOM(obj1,obj2)$ is either 0 or 1, i.e. $RECOM(obj1,obj2) \in \{0,1\}$.

A. Trust evaluation algorithm

In order to compute the trust value of the user to an object, we use a time window $[T_0,T_n]$, and split $[T_0,T_n]$ into n non-overlapping slices. Let the k-th event in the i-th time slice be denoted as e_k^i. If an event is a positive trust, then its value is 1, and otherwise, the value is -1. Let S_{AB} be the number of positive events, and F_{AB} be the number of negative events, then the trust value $TRUST(A,B) = \frac{S_{AB}}{S_{AB}+F_{AB}}$.

In a time window, the events are mutual independent, and thus all events are independently and identically distributed. In the time slice $[T_i,T_{i+1}]$, the event sequence is $V_i = \{v_1^i, v_2^i, .., v_n^i\}$. Let the probability of $v_k^i = 1$ be p, i.e. $P(v_k^i = 1) = p)$, then $P(v_k^i = -1) = 1-p)$. So, $V_i \sim B(1,p)$, and the distribution of $v_1^i, v_2^i, .., v_n^i$ is $p^x(1-p)^{n-x}$, where $0 \le x \le n$. Let the prior of p be $h(p)$, then according to the Bayesian rule the posterior is

$$h(p \mid v_1^i, v_2^i, .., v_n^i) = \frac{h(p)p^{S_{AB}}(1-p)^{F_{AB}}}{\int_0^1 h(p)p^{S_{AB}}(1-p)^{F_{AB}}\,\mathrm{d}p} \quad (1)$$

Where $0 \le p \le 1, S_{AB} + F_{AB} = n$.

As the distributions of trusts from different directions between two objects are the same, i.e. $h(p)$ is uniformly distributed, then we have

$$h(p \mid v_1^i, v_2^i, .., v_n^i) = \frac{p^{S_{AB}}(1-p)^{F_{AB}}}{\int_0^1 p^{S_{AB}}(1-p)^{F_{AB}}\,\mathrm{d}p} \quad (2)$$

Where $0 \le p \le 1$, $S_{AB} + F_{AB} = n$.

From equation 2 we can see that, $h(p \mid v_1^i, v_2^i, .., v_n^i)$ conforms to the β distribution. We use the expectation of its posterior, i.e. $E(p \mid v_1^i, v_2^i, .., v_n^i)$, as the estimation of p, then we have

$$p(v_1^i, .., v_n^i) = \int_0^1 p \cdot h(p \mid v_1^i, .., v_n^i)\mathrm{d}p = \frac{S_{AB}+1}{n+2} \quad (3)$$

Because future behavior is predicted based on history, we use the trust history of object A on object B to estimate the future behaviour of A trusting on B, then we have

$$TRUST_{\text{direct}}^i(A,B) = \frac{S_{AB}+1}{S_{AB}+F_{AB}+2}. \quad (4)$$

While normalizing the trusts of all events in time slice j, we can get

$$I_j = \begin{cases} 0 & \text{if } !\exists e_k \in [t_{j-1}, t_j] \\ \dfrac{\sum_{k=1}^{n_j} v_k^j}{\sum_{k=1}^{n_j} \mid v_k^j \mid} & \text{otherwise} \end{cases} \quad (5)$$

Then the final trust probability of A on B is

$$TRUST_{\text{direct}}(A,B) = \sum_{i=1}^{n} \frac{I_i}{n} \quad (6)$$

B. Penalty mechanism

In an open environment, there is one kind of objects, which hide in the system for a long time to accumulate very high trustiness, and then do some hostile actions. So,

in order to deal with this problem, we introduce a penalty mechanism. The penalty mechanism is based on congestion control of TCP protocol. We set a slide window in the mutual sequence of two objects, sample the positive and negative events from the slide window, and then compute the trust probability according to the recent mutual information. So, an object can recognize the hostile actions of other objects.

The penalty mechanism is illustrated in figure 2. We first set an adjustable slide window in the sequence of object interactions. Let the slide window in the sequence of interactions between A and B be W_{AB}, then the control of the slide window between A and B is described in figure 2.

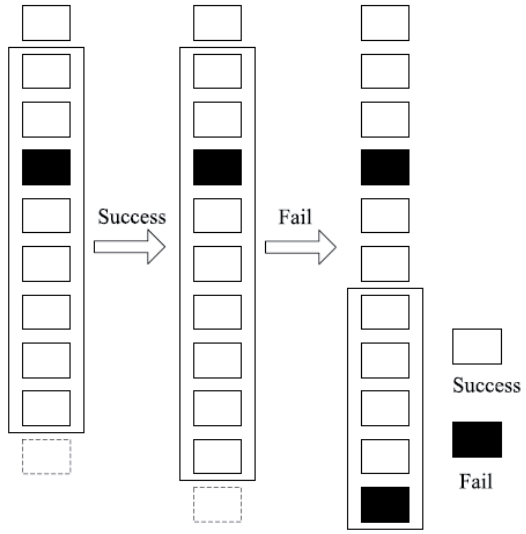

Figure 2. Model of the slide window

Let the threshold of the size of the slide window be ξ. At the beginning, the size of the slide window is $W_{AB} = 0$. In the mutual evaluation of two objects, if an interaction is a positive event, then if $W_{AB} < \xi$, $W_{AB} = W_{AB} + 1$, otherwise, $W_{AB} = \xi$; and if an interaction is a negative event, then $W_{AB} = W_{AB} / 2$.

In order to present the trust relationship between two objects directly, we introduce the concept of mutual fault rate. The mutual fault rate is the percent of faults (or failures) in the recent slide window, and its value is

$$\eta = \frac{F_{AB}}{W_{AB}}. \tag{7}$$

When a fault is occurred, W_{AB} decreases exponentially, η increases rapidly, and then both sides of authentication could know the recent trust status of the other side sensitively. When the interaction is successful, W_{AB} increases linearly, and then η increases slowly. The above mechanism can make increase and decrease of η in different speed, which is more suitable to the trust mechanism in people's usual life. In general, if W_{AB} decreases, then η will increase exponentially, but in the congestion control of TCP control protocol, the size of the slide window will be concussive.

Figure 3 is an example of concussive situation in a slide window. Before the interaction of two objects, let $\eta = \frac{1}{3}$, and when a negative trust occurs, $\eta = \frac{1}{5}$. However, the true value of η should increase after a negative interaction. The reason is that hostile object alternates between positive and negative interactions, which can cheat the other object while interacts with another object.

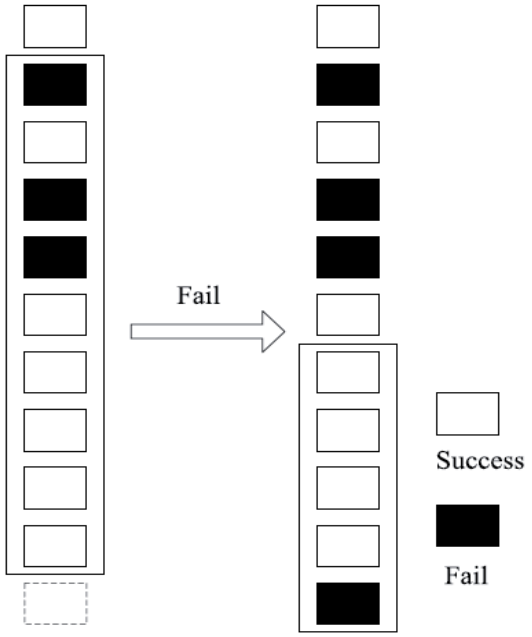

Figure 3. Concussive interaction in a slide window

In order to penalize this kind of hostile objects, we introduce the method in TCP congestion control protocol. When η decreases because of reduction of size of the slide window, a concussive interaction occurs. Let the concussive factor is denoted as μ, and initiate it with $\mu = 0$, then the value of μ updates continuously, the update equation is as follows:

$$\mu = \begin{cases} \mu + \eta(n-1) - \eta(n) & \text{if } \eta(n) < \eta(n-1) \\ \mu & \text{otherwise} \end{cases}, \tag{8}$$

Where $\eta(n)$ is the mutual fault rate after the slide window contracts, and $\eta(n-1)$ is the mutual fault rate before the slide window contracts.

This concussive interaction reflects the unreliability of objects, and is called inconstancy in people's usual life, so we revise the number of faults as follows:

$$F_{AB} = (1+\mu)F_{AB}. \tag{9}$$

Finally, after introducing the mutual fault rate, computation of trust value described in equation 4 and 6 can be rewrote as

$$TRUST^{i}_{\text{direct}}(A,B) = \frac{S_{AB}+1}{S_{AB} + (1+\mu)F_{AB} + 2}, \tag{10}$$

$$\text{and } TRUST_{\text{direct}}(A,B) = (1-\mu)\sum_{i=1}^{n}\frac{I_i}{n} \quad (11)$$

C. Trust recommendation evaluation algorithm

Here, we denote the recommendation trust [27] as the dependence of object A on object B, i.e. $Tr(A,B)$. From the viewpoint of A, the recommendation trust from B can be computed by their common evaluations to other objects. If A wants to interact with C, it get recommendation trust value $D(B,C)$ from B, and when the interact is over, the evaluation of A on C is $D(A,C)$, then evaluation similarity between A and C is

$$\theta = \min\left(\frac{D_{(A,C)}}{D_{(B,C)}}, \frac{D_{(B,C)}}{D_{(A,C)}}\right). \quad (12)$$

According to [27], the recommendation trust can be computed as follows:

$$T_{r(A,B)}^{k+1} = (1-r)T_{r(A,B)}^{k} + \gamma\theta \quad (13)$$

Where γ is the tradeoff coefficient and θ is the evaluation similarity between A and B. The value of γ depends on the interactions between A with B, and the more the number of interactions, the bigger.

In order to prevent the affect of hostile objects on evaluations, we introduce loyalty into the computation of recommendation trust, and the loyalty including recommendation and target objects can be computed as follows:

$$\text{lo}\,yalty(r_k) = \begin{cases} 1 & if\ \dfrac{I_k(A_i,B)}{I_{cur}(A,B)} \le 1 \\ \dfrac{P_k(A_i,B)I_k(A_i,B)}{I_{cur}(A,B)} & otherwise \end{cases} \quad (14)$$

Where $I_k(A_i,B)$ is the importance of the k-th interaction between A with B, and $P_k(A_i,B)$ is the expectation of future interactions in the k-th interaction. So, the recommendation trust can be revised as follows.

$$TRUST_{indirect}(A_i,B) = T_{r(A_i,B)}^{k} \times Loyalty(r_k) \quad (15)$$

In the open environment, when computing the evaluation of A on B, we need to take both direct and indirect recommendation trusts into consideration, so the final trust recommendation evaluation is

$$TRUST(A,B) = \varepsilon_1 TRUST_{direct}(A,B) + \varepsilon_2 TRUST_{indirect}(A,B) \quad (16)$$

Where $\varepsilon_1 > 0$, $\varepsilon_2 > 0$, and $\varepsilon_1 + \varepsilon_2 = 1$. In general, with the increase of interactions with other objects, the direct trust is more and more important, so ε_1 becomes bigger and bigger, and ε_2 becomes smaller and smaller.

IV. EXPERIMENTS

In the experiments, we apply the NS2 network simulation toolkit to simulate a wireless sensor network, and the baseline algorithms are NDAS [8], LCSS [9] and SEDR [15].

A. Experimental setup

In a region of 1200×1200, we randomly place 100 sensors, and these sensors form a wireless sensor network. We let the number of hostile sensors be $k=1$ or $k=2$, and other parameters of the sensor network are in table 1.

TABLE I.
TABLE OF PARAMETER SETTING

Parameters	Values
sensor communication radius/m	10
length of data package/Byte	4000
running time/s	100
shared secret key package length/bit	200
sub secret key package length/bit	10

B. Experimental results

We let the number k of hostile nodes be 1 and 2 respectively, and observe the probabilities that hostile nodes are recommended to a source node. We compare our approach to the NDAS algorithm under the above situations and the result are in figures 4 and 5 respectively. In these two figures, the horizontal axis is the number of nodes in the experiments, and the vertical axis is the probability that a recommendation trust is from hostile node. From these two figures we can see that, when the scale of network increases, the probabilities decrease in both algorithms. In addition, our proposed approach is obviously better than the NDAS algorithm.

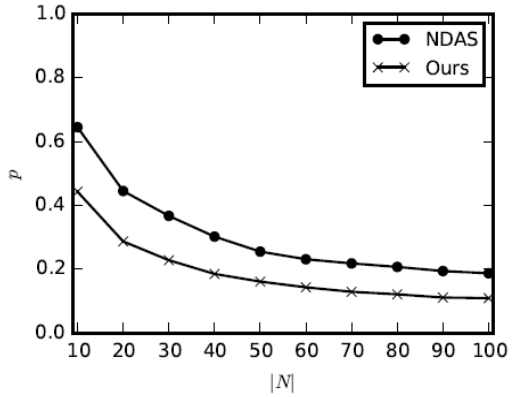

Figure 4. Probabilities of hostile nodes recommended, $k=1$

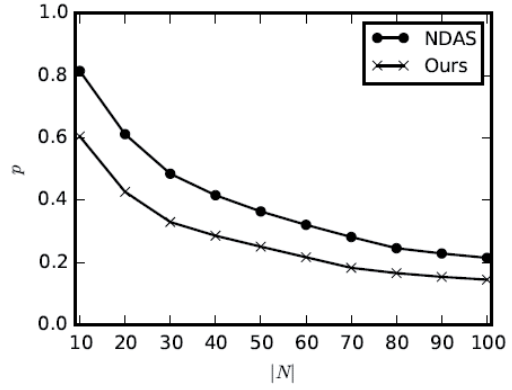

Figure5. Probabilities of hostile nodes recommended, $k=2$

We compare the transmission rates of algorithms between the proposed approach with NDAS, SEDR and LCSS. Figure 6 illustrates the transmission rates (or communication) of different algorithms along with time, and the time interval is 10 seconds. As time goes on, the transmission rates of all algorithms decrease appreciatively, but our proposed approach has the least transmission rate. This means that, in order to deal with authentication efficiently our approach needs least transmitted data, and this can reduce energy consumption and the time required by authentication. So, it is more suitable to sensor networks.

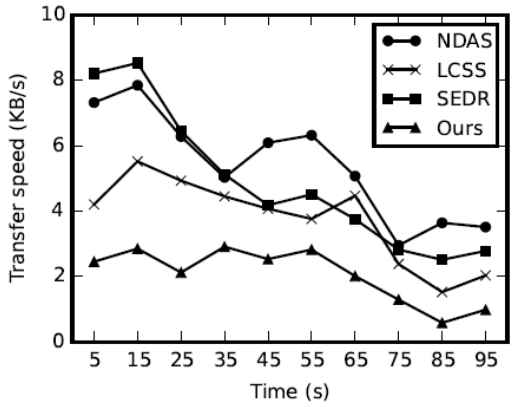

Figure 6. Comparison of communication

Table II illustrates the comparison of communication data packages of the four algorithms in a certain situation. From these experimental data we can see that, our approach has the least communication packages, so it can reduce communication overhead on the sensor network, and thus relieve the network congestion. This is the reason why we choose the TCP congestion control protocol.

TABLE II.
COMPARISON OF COMMUNICATION DATA PACKAGES

Algorithms	#send	#receive	receive/send	#transfer
	packages	packages	rate	packages
NDAS	1159	5172	4.463	71477
SEDR	1155	4921	4.256	76539
LCSS	1052	4423	4.202	66645
Ours	855	3305	3.860	40669

Table III illustrates the comparison of running time in one authentication period of the four algorithms. A authentication period includes the time for building shared secret key and the time for finishing one authentication, and its unit is nanosecond. From these data we can see that, our approach needs less than a half of time than any other algorithm in both building shared secret key time and authentication time.

TABLE III.
COMPARISON OF RUNNING TIME

2*Algorithms	Running time (ns)	
	building key time	*authorization time*
NDAS	1159	5172
SEDR	1155	4921
LCSS	1052	4423
Ours	855	3305

Table IV illustrates the comparison of maximal memory usages of the four algorithms. The ratio in table 4 is the ratio of memory usage of each algorithm to the memory usage of our proposed approach. The other three algorithms use about 1.7 to 2 times of memory compared with our approach, The reason is that we apply slide window to capture the interaction history, and this needs less memory.

TABLE IV.
COMPARISON OF MEMORY USAGE

Algorithms	Memory usage/MB	Ratio
NDAS	56.59	1.933
SEDR	57.90	1.977
LCSS	51.42	1.756
Ours	29.68	1

V. CONCLUSION

In this paper, we study the authentication mechanism in wireless sensor networks based on trust. The recommendation trust of a source object to a target object comes from their common access to other objects, and this can be computed using the interaction history between objects. In order to further improve the efficiency of the approach, we apply the slide window technique to capture the interaction history between objects. The simulating experiments validate the efficiency and effectiveness of the proposed approach.

REFERENCES

[1] Chaudhari, H., Kadam, L.: Wireless sensor networks: security, attacks and challenges. International Journal of Networking 1(1), 4–16 (2011)

[2] Othman, M.F., Shazali, K.: Wireless sensor network applications: A study in environment monitoring system. Procedia Engineering 41, 1204–1210 (2012) http://dx.doi.org/10.1016/j.proeng.2012.07.302

[3] Al Ameen, M., Liu, J., Kwak, K.: Security and privacy issues in wireless sensor networks for healthcare applications. Journal of medical systems 36(1), 93–101 (2012) http://dx.doi.org/10.1007/s10916-010-9449-4

[4] Aziz, A.A., Sekercioglu, Y.A., Fitzpatrick, P., Ivanovich, M.: A survey on distributed topology control techniques for extending the lifetime of battery powered wireless sensor networks. Communications Surveys & Tutorials, IEEE 15(1), 121–144 (2013) http://dx.doi.org/10.1109/SURV.2012.031612.00124

[5] Duriˇsi´c, M.P., Tafa, Z., Dimi´c, G., Milutinovi´c, V.: A survey of military applications of wireless sensor networks. In: Embedded Computing (MECO), 2012 Mediterranean Conference On, pp. 196–199 (2012). IEEE

[6] Xia, F., Yang, L.T., Wang, L., Vinel, A.: Internet of things. International Journal of Communication Systems 25(9), 1101 (2012) http://dx.doi.org/10.1002/dac.2417

[7] Jain, A., Kant, K., Tripathy, M.: Security solutions for wireless sensor networks. In: Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference On, pp. 430–433 (2012). IEEE http://dx.doi.org/10.1109/acct.2012.102

[8] Dubrova, E., Naslund, M., Seiander, G., Tsiatsis, V.: Energy-efficient message authentication for ieee 802.15. 4-based wireless sensor networks. In: NORCHIP, 2014, pp. 1–4 (2014). IEEE

[9] Gao, Y., Zeng, P., Choo, K.-K.R.: Multi-sender broadcast authentication in wireless sensor networks. In: Computational Intelligence and Security (CIS), 2014 Tenth International Conference On, pp. 633–637 (2014). IEEE

[10] Kumar,v., Jain, A., Ovsthus, K., Kristensen, L.M.;An industrial perspective on wireless sensor networks-a survey of requirements, protocols, and challenges. Communications Surveys & Tutorials,

IEEE 16(3), 1391–1412 (2014) http://dx.doi.org/10.1109/SURV.2014.012114.00058

[11] Kumar, V., Jain, A., Barwal, P.: Wireless sensor networks: Security issues, challenges and solutions. International Journal of Information & Computation Technology. ISSN, 0974–22394 (2014)

[12] Pankanti, S., Bolle, R.M., Jain, A.: Biometrics: The future of identification [guest eeditors' introduction]. Computer 33(2), 46–49 (2000) http://dx.doi.org/10.1109/2.820038

[13] Bicego, M., Lagorio, A., Grosso, E., Tistarelli, M.: On the use of sift features for face authentication. In: Computer Vision and Pattern Recognition Workshop, 2006. CVPRW'06. Conference On, pp. 35–35 (2006). IEEE http://dx.doi.org/10.1109/cvprw.2006.149

[14] Yang, W., Hu, J., Wang, S.: A delaunay triangle-based fuzzy extractor for fingerprint authentication. In: Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference On, pp. 66–70 (2012). IEEE http://dx.doi.org/10.1109/trustcom.2012.23

[15] Banerjee, S., Mukhopadhyay, S., Rondoni, L.: Multi-image encryption based on synchronization of chaotic lasers and iris authentication. Optics and Lasers in Engineering 50(7), 950–957 (2012) http://dx.doi.org/10.1016/j.optlaseng.2012.02.009

[16] Scheidat, T., K¨ummel, K., Vielhauer, C.: Short term template aging effects on biometric dynamic handwriting authentication performance. In: Communications and Multimedia Security, pp. 107–116 (2012). Springer http://dx.doi.org/10.1007/978-3-642-32805-3_9

[17] Choi, S., Youn, I.-H., LeMay, R., Burns, S., Youn, J.-H.: Biometric gait recognition based on wireless acceleration sensor using k-nearest neighbor classification. In: Computing, Networking and Communications (ICNC), 2014 International Conference On, pp. 1091–1095 (2014). IEEE

[18] Sprager, S., Juric, M.B.: Inertial sensor-based gait recognition: A review. Sensors 15(9), 22089–22127 (2015) http://dx.doi.org/10.3390/s150922089

[19] Patel, S.N., Pierce, J.S., Abowd, G.D.: A gesture-based authentication scheme for untrusted public terminals. In: Proceedings of the 17th Annual ACM Symposium on User Interface Software and Technology, pp. 157–160 (2004). ACM http://dx.doi.org/10.1145/1029632.1029658

[20] Lai, K., Konrad, J., Ishwar, P.: Towards gesture-based user authentication. In: Advanced Video and Signal-Based Surveillance (AVSS), 2012 IEEE Ninth International Conference On, pp. 282–287 (2012). IEEE

[21] Farella, E., O'Modhrain, S., Benini, L., Ricc´o, B.: Gesture signature for ambient intelligence applications: a feasibility study. In: Pervasive Computing, pp. 288–304. Springer, (2006) http://dx.doi.org/10.1007/11748625_18

[22] Liu, J., Zhong, L., Wickramasuriya, J., Vasudevan, V.: User evaluation of lightweight user authentication with a single tri-axis accelerometer. In: Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services, p. 15 (2009). ACM http://dx.doi.org/10.1145/1613858.1613878

[23] Okumura, F., Kubota, A., Hatori, Y., Matsuo, K., Hashimoto, M., Koike, A.: A study on biometric authentication based on arm sweep action with acceleration sensor. In: Intelligent Signal Processing and Communications, 2006. ISPACS'06. International Symposium On, pp. 219–222 (2006). IEEE http://dx.doi.org/10.1109/ispacs.2006.364871

[24] Matsuo, K., Okumura, F., Hashimoto, M., Sakazawa, S., Hatori, Y.: Arm swing identification method with template update for long term stability. In: Advances in Biometrics, pp. 211–221. Springer, (2007) http://dx.doi.org/10.1007/978-3-540-74549-5_23

[25] Liu, J., Zhong, L., Wickramasuriya, J., Vasudevan, V.: uwave: Accelerometer-based personalized gesture recognition and its applications. Pervasive and Mobile Computing 5(6), 657–675 (2009) http://dx.doi.org/10.1016/j.pmcj.2009.07.007

[26] Perrig, A., Stankovic, J., Wagner, D.: Security in wireless sensor networks. Communications of the ACM 47(6), 53–57 (2004) http://dx.doi.org/10.1145/990680.990707

[27] Chen, T.-Y., Chen, Y.-M., Lin, C.-J., Chen, P.-Y.: A fuzzy trust evaluation method for knowledge sharing in virtual enterprises. Computers & Industrial Engineering 59(4), 853–864 (2010) http://dx.doi.org/10.1016/j.cie.2010.08.015

AUTHOR

Ru-ping Li is with the Department of Electronic Information, Anhui Business Vocational College, 231131 Hefei City, Anhui Province, China (lrp15@163.com).

This work was supported by the Key project of natural science research in Anhui Universities (KJ2015A389, KJ2015A450); the Key project of Discipline (professional) talents academic funding in Anhui Universities (gxbjZD2016094)Submitted 26 October 2015. Published as resubmitted by the author 23 December 2015.