ATLANTIS PRESS

Advances in Engineering Research, volume 118

2nd International Conference on Automation, Mechanical Control and Computational Engineering (AMCCE 2017)

Security Analysis of the Authentication Schemes Based on Wireless Sensor Networks

Binbin Yu[1,2, a], Liang Hu[1,b]

[1]College of Computer Science and Technology, Jilin University, Changchun, 130012, China.

[2]College of Information Technology and Media, Beihua University, Jilin, 132013, China.

[a]164504108@qq.com, [b]hul@mails.jlu.edu.cn

Keywords: Wireless sensor network; identity authentication; key agreement; attack.

Abstract. As one of the basic technologies for building Internet of Things, wireless sensor networks (WSNs) are a hot research topic at present. In this paper, two basic structures of WSNs are described briefly, and the current security situation and security risks of WSNs are introduced. Then, this paper summarizes several mainstream ways of attacking identity authentication schemes that are applied to WSNs, including smart card theft, wireless sensor node capture, vampire attack and collusion attack, and presents some defensive measures. Finally, attacking principles of these attack methods are summarized, and some improvements are put forward.

1. Introduction

WSNs are a kind of special Ad-Hoc networks composed of a large number of wireless sensor nodes with sensing, wireless communication and micro-processing capabilities [1] [2]. In general, the wireless sensor nodes use the long-distance communication technology to indirectly or directly transmit the data perceived to the monitoring center via the cluster head nodes by means of multi-hop relay, thereby completing the tasks assigned by the users or monitoring center [3][4]. Compared to the traditional communication networks with fixed infrastructure, WSNs have a very strong self-organization mechanism because of its Ad-Hoc network characteristics. Moreover, its system survivability and flexibility are also stronger than the traditional networks. Compared to the Ad-Hoc networks, WSNs have a lower overall data processing capability because of the rather limited processing power and storage capacity of wireless sensor nodes. However, the distribution scale and the number of deployable wireless sensor nodes of WSNs are far beyond the Ad-Hoc networks, which greatly enhance their data collection capability. Therefore, the application range of WSNs is becoming increasingly extensive, and related research fields have also become one of the hotspots at present [5][6][7]. Security system, which guarantees the stable and normal operation of the WSN system, is an important part of WSNs.

Security system of WSNs somewhat varies as the WSNs themselves have limitations: 1. The majority of wireless sensor nodes are distributed in the areas difficult to reach by humans, that is, wireless sensor nodes can easily be captured; 2. Wireless sensor nodes are not required to carry computationally complex protocols with high energy consumption due to their own limitations in processing ability, storage capacity and power. 3. The peculiarity of wireless network information transmission, i.e. wireless transmission, means that the information being transmitted can be intercepted, replayed or tampered, which pose great threats to the information security of WSNs [8][9].

As an integral part of the security architecture of WSNs, the identity authentication system plays an important role in identifying and preventing malicious attackers, managing access rights and protecting privacy protection [10][11]. With the deepening of research, the identity authentication system can also prevent the denial of service attacks [12], wormhole attacks and other common attacks to some extents. This paper focuses on studying the mainstream identity authentication

schemes and analyzes their structure and characteristics. Meanwhile, several popular effective attack methods are also studied, and corresponding security improvements are proposed for these attacks.

2. Current security situation of WSNs

Depending on the mode of transmission, WSNs are generally organized in two forms [13][14]: In the first form, each wireless sensor node directly transmits the data information collected to the data center. Such WSNs have relatively simple composition, where various sensor nodes are the same in function, and the entire network is not hierarchical. As the data collected are transmitted directly to the data center, the energy consumed for computation and data transmission are relatively large for each sensor node.

In the second form, each sensor node indirectly transmits the data information collected to the data center through the cluster head nodes. Under such a mode, the WSN allocates a cluster head node for each cluster of wireless sensor nodes according to the distributed region. Cluster head nodes have performance far superior to the ordinary nodes. The data information collected by all wireless sensor nodes within the responsible region of a cluster head node is transmitted to the data center via the cluster head node. For such WSNs, each ordinary wireless sensor node only needs to have the simple processing ability, transmission capacity and battery reserve to complete the tasks the same as the sensor nodes in the first network. Its operation mode is as shown in Figure 1.

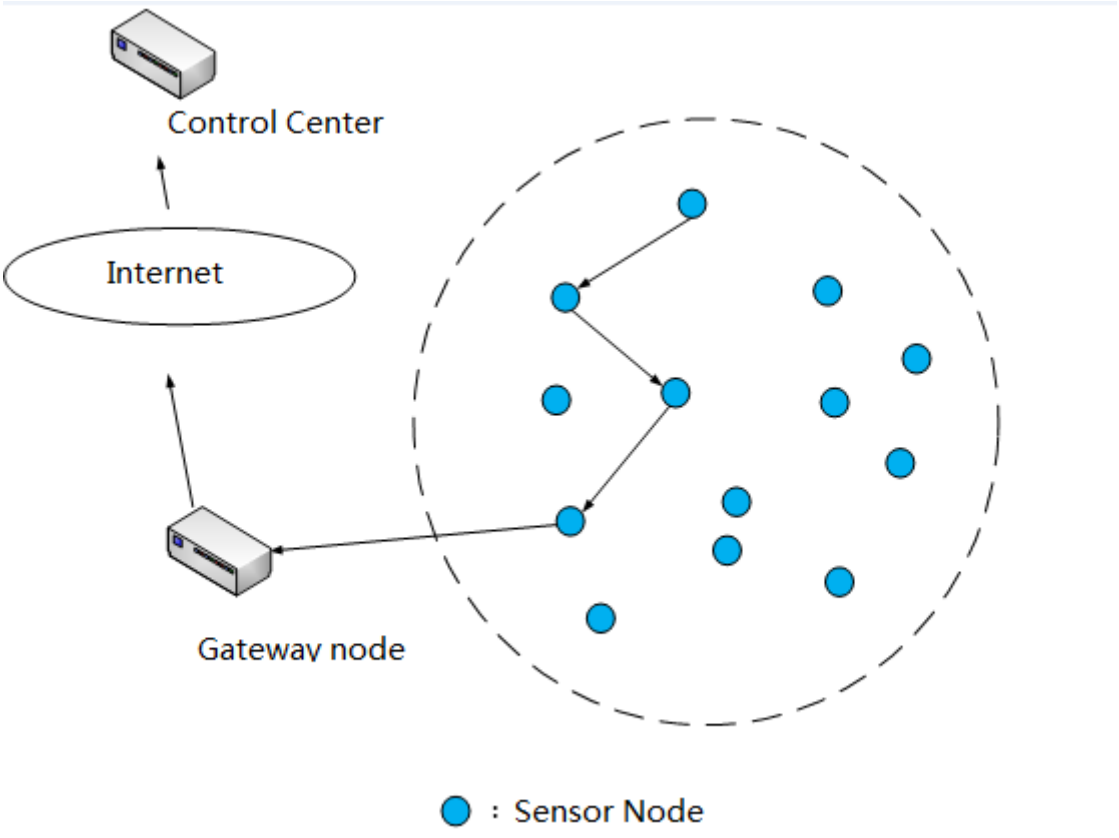

Figure 1 Structure diagram of WSNs

Given the above different compositions of WSNs, the design idea of WSN-based identity authentication scheme also varies, which can be categorized according to the actual participants in the schemes into: the two-party identity authentication schemes and the three-party identity authentication schemes [15][16]. Two-party identity authentication schemes are basically used for WSNs in which the wireless sensor nodes directly transmit data to the data center. In such WSNs, the

participants are usually node–node or node–service user (user). Three-party identity authentication schemes, on the other hand, are used mainly for WSNs in which the sensor nodes indirectly transmit data information to the data center via cluster head nodes. For a few WSNs used for the sensor nodes to directly transmit data to the data center, the participants are usually node–cluster head node–data center, node–cluster head node–user, node–registered data center–roaming data center. Figure 2 presents a classic three-party identity authentication scheme, where MS represents the sensor node; VLR represents the roaming data center; and HLR represents the registered data center.

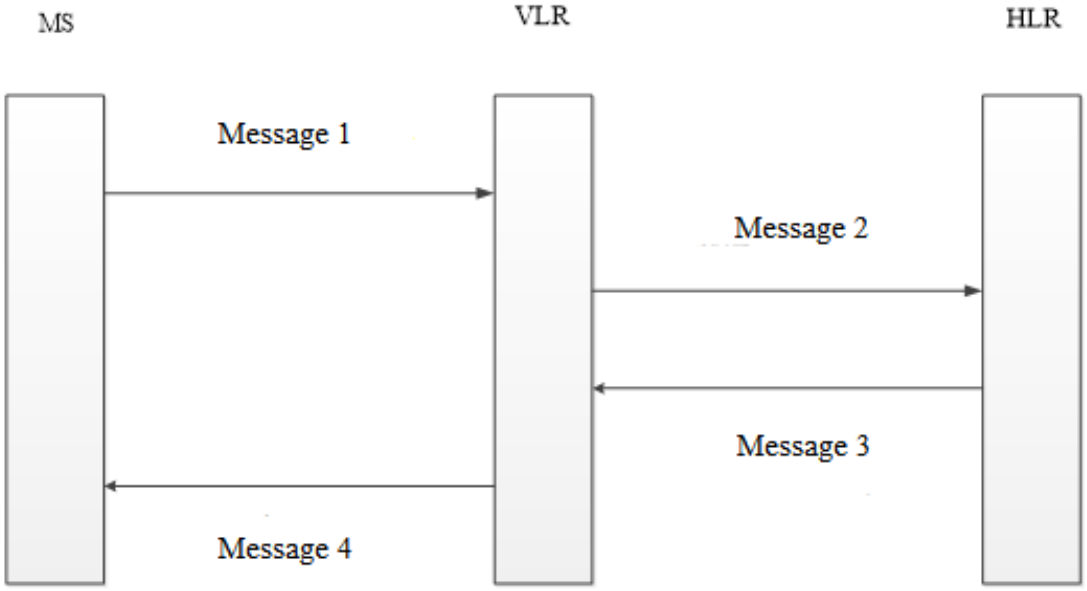

Figure 2 Three-party identity authentication scheme

2.1 Security requirements of WSNs

Before understanding the specific scheme of identity authentication, it is necessary to understand the security requirements of WSNs [17], which are also a prerequisite for designing excellent identity authentication schemes:

(1) Availability: WSNs or wireless sensor nodes can still continue normal and stable operation under any malicious attack by adversaries.

(2) Confidentiality: The information transmitted in a WSN must maintain the necessary confidentiality. Even if the information in transit or stored in the device is eavesdropped, intercepted or stolen by the adversaries, it can be ensured that the sensitive information is not easily decrypted.

(3) Integrity: It should be ensured that the information in transit and the data information received by each wireless sensor are all complete, rather than tampered, deleted by adversaries or incomplete for other reasons.

(4) Legitimacy of identity: The legitimacy of identities must be mutually verified between the wireless sensor nodes; nodes and users; and nodes and data center, in order to prevent the masquerading attacks (fake nodes, fake users, etc.) by adversaries. The legitimacy of the information sent and received by any party must be ensured, as well as the identity legitimacy of the information source, in order to prevent receipt of information that has been tampered with by adversaries.

(5) Non-repudiation: Any participant in an identity authentication scheme must be responsible for the information it sends, that is, the sender of data information cannot deny the information it sent, while the receiver of data information can confirm the sender of the data information through the information received.

2.2 Security risks of WSNs

The security risks faced by WSNs should also be considered before designing any identity authentication scheme. This paper mainly considers the security risks above the physical layer, while the security risks of physical layer are not discussed much [18].

(1) Data link layer: Security risks faced by the data link layer are primarily resource consumption attacks, of which denial of service (DOS) attacks are one of the most typical attack types. Attackers substantially consume the WSNs' bandwidth, memory, CPU, battery power and the like using DOS attacks, thereby seriously disrupting the normal operation of WSNs.

(2) Network layer: Security threats faced by the network layer are mainly replay attacks, black hole attacks and collusion attacks.

There are two major types of replay attacks. One type is the sending delay replay attacks where the data information is not tampered with. Such attacks are usually used for implementing masquerading attacks. For example, an adversary may imitate a legitimate user through a replay attack after intercepting the identity authentication information sent by the legitimate user to the sensor node, thereby gaining the trust of the sensor node. The other type is the replay attacks where the data information is partially tampered with. Such attacks are mostly used for forgery attacks. For example, an adversary tampers with the identity information in the identity authentication information sent by a legitimate user to the sensor node after intercepting it, then replaces it with his own identity, thereby pretending himself as a legitimate user to gain the trust of the sensor node.

Black hole attack refers to that the attacker lures other wireless sensor nodes to send packets to it, thereby constructing an attacker-centered "black hole". The typical attack pattern is to let other nodes believe that the attacker is the best forwarding route option according to the existing routing algorithm of WSNs, thereby attracting these nodes to send packets to it.

Collusion attack is a new type of attack against WSNs, where a "traitor" is inserted into the WSNs to help the external adversary launch attacks against the WSNs.

(3) Transport layer: Flooding attacks are the primary considerations in this layer, where the attackers send a large number of attack packets to degrade the performance of entire network and disable normal communication. Similar to DOS attacks, flooding attacks are also designed to drain the network resources of WSNs.

3. Several major attack methods

3.1 Smart card theft attacks

In WSNs, the information of legitimate users is also one of the protection goals of security system. The user information mainly includes identity information, login password and other sensitive information. Before the widespread use of smart cards, these sensitive information were preserved by users themselves, which easily led to errors during user input of information. Moreover, in case of accidental loss, it would cause a great threat to the WSNs. With the development of hardware technology, the algorithms and systems on the wireless sensor nodes are becoming increasingly complex, and the attack pattern has also presented diversity. So preservation of confidential information by users alone is no longer adequate. Hence, the current identity authentication and key management schemes all choose to store some confidential information of users on the smart card with certain computing and processing capabilities.

The original smart cards, similar to the nowadays bank cards, only stored part of the user confidential information on them. When the user wanted to use the services provided by WSN, they needed to insert their smart cards in the terminal first, then enter the identity information and password to log in to the WSN. Today's smart cards not only can achieve the foregoing functions, but also possess certain computing, storage and processing capabilities. Some parameters used in the identity authentication and key management schemes can be completed on the smart cards.

In a scheme proposed by Turkanovic et al. [19][20], if an adversary obtains the smart card of a legitimate user U by means of theft or the like and cracks the card through violence and other means, it means that the adversary gains the sensitive information {*M,e,f*} held by this legitimate user in the smart card. Using these sensitive information, the adversary can launch the masquerading attack under certain conditions. The adversary can use the confidential information {*M,e,f*} obtained to normally log in to the WSN. The attack procedure is as follows:

(1) The adversary sends the confidential information {*M,e,f*} obtained to the wireless sensor node with which he wants to communicate.

(2) The wireless sensor node cannot distinguish whether the source of information is a real legitimate user, but it believes that the gateway node GW will help it. So the information is normally sent to the GW.

(3) However, actually GW is also unable to tell whether the source of information is a real legitimate user and will authenticate the information as correct. Hence, the adversary successfully logs in to the WSN and accesses to the wireless sensor node services.

3.2 Wireless sensor node capture attacks

Wireless sensor nodes are easily captured as they are distributed mostly in the unmanned or adversary-controlled areas. Once the wireless sensor node is captured, the adversary can decrypt the confidential information stored in the wireless sensor node through violence and other means. After obtaining these confidential information, the adversary can launch further attacks by exploiting the aforementioned smart card theft attacks, such as masquerading attacks, so that the illegal node can join the WSN as a legitimate node, or that an illegal user can access to the WSN as a legitimate user to get legitimate services. When combined with collusion attacks, an illegal user can even acquire legal status to become a legitimate user, who can access to the resources and data provided by the WSN.

Again taking the scheme proposed by Turkanovic et al. as an example, if an adversary captures a legitimate wireless sensor node S and decrypts the confidential information stored on it through violence and other means, who can normally use this wireless sensor node S through monitoring and other means and is able to obtain information stored in S in real time. Then, the adversary can place this wireless sensor node S back to its original location and wait for legitimate users to contact it. This way, when the legitimate users Ul contact the wireless sensor node S, the adversary can let them continue normal communication. When the communication proceeds to the fourth step, the adversary can obtain the confidential information *{M,e,f}* of the user U through the information obtained by decoding node S, as well as the communication information between U and S obtained by interception.

3.3 Vampire attacks

Vampire attacks can be regarded as a variant of resource consumption attacks [21][22]. By substantially increasing the packet transmission frequency between wireless sensor nodes, the adversary consumes the computing resources and battery power of the nodes. This will greatly reduce the service life of the wireless sensor nodes. Moreover, as the messages in transit are all legitimate messages, the processing and storage resources of wireless sensor nodes are seriously occupied, thereby resulting in serious waste of resources.

By altering the routing protocol of wireless sensor nodes, the adversary screens some settings that can be changed through studying the routing and gateway protocols used by the wireless sensor nodes. This way, after changing these settings, the frequency of data forwarding between some of the normal wireless sensor nodes will increase. According to experiments, vampire attacks can increase the power consumption of WSNs by 50%-1000% under different experimental environments. The simpler the structure of deployed wireless sensor nodes themselves, the greater the destructive power of vampire attacks.

3.4 Collusion attacks

Collusion attacks are a new type of effective attack method [23][24], which attacks the target mainly by trying all means to turn a legitimate participant into a "traitor" within the attacking target. The wireless sensor node capture attacks in section 2.2 are also one commonly used "traitor" insertion method of the collusion attacks. It compromises a legitimate wireless sensor node by capturing it, then normally use the compromised node without changing the confidential information stored inside it while knowing these confidential information. Attack pattern is usually to let the illegal nodes or users join the WSNs by compromising a node, or to compromise partial confidential information of a node to decrypt the session key between other nodes, thereby obtaining the sensitive information in transit.

Taking the scheme proposed by Turkanovic et al. again as an example, the adversary obtains the confidential information {*M,e,f*} of a legitimate user U with the help of the wireless sensor node capture attacks mentioned in section 2.2. Using this information, the adversary can log in to other wireless sensor nodes to obtain their services. The procedure is as follows:

(1) When a user U wishes to contact another wireless sensor node S1, the adversary can immediately transmits the intercepted request information to its target wireless sensor node S2.

(2) As the wireless sensor node cannot distinguish whether the source of this request information really wants to contact it, and as the request information is legal, S2 continues to execute subsequent operation. After completion of the operation, S2 sends an acknowledgment message to the source of information request, i.e. the legitimate user U.

(3) After an adversary intercepts the acknowledgment message sent by S2 to U, he can use the confidential information {*M,e,f*} obtained before to get the session key between S2 and U, which means that the adversary can masquerade as the legitimate user U to communicate with the wireless sensor node S2.

Tang et al. proposed a classic three-party identity authentication and key management scheme for WSNs [25], by which the whole authentication process can be completed only by needing four communications. However, there are still security risks when facing the collusion attacks.

Consider the following scenario:

Since the key ck is decided by the timestamp and temporary parameters, that is, ck has already been generated after the information S1 is sent. Assuming that the adversary can eavesdrop all the information sent and received by node MS, and that the adversary controls a VLR with a legal identity as the "traitor", which is called VLR' with an identity of IDV'.

(1) After interception of information S1, the VLR' establishes a session key $K_{V,H}^{'}$ with the MS's registered base station HLR to contact with the HLR. According to the identity IDM and confidential information m_w of wireless sensor node, VLR' produces a message S2' the same as that should be sent by VLR and sends it to the HLR before VLR. Obviously, HLR can correctly decrypt the received message S2' to obtain the ck contained therein. HLR can also verify the correctness of the temporary parameters and electronic certificate correctly. Afterwards, HLR uses $K_{V,H}^{'}$ to generate an encrypted message $\left\lfloor IDM, T_{\exp}, ts, ck, N \right\rfloor_{K_{V,H}^{'}}$, then constitutes a message S3' and sends it to the VLR'.

(2) After receiving S3', the adversary-controlled VLR' can correctly decrypt the secret key ck and other confidential information with $K_{V,H}^{'}$, definitely without needing to continue to send S4 to the MS. At this time, MS and VLR on the other side have also completed mutual authentication, where the key ck becomes the session key between them.

Based on the scheme proposed by Tang et al., Chang et al. put forward an improved scheme ASMAS with anonymity [26]. The scheme presented some shortcomings of EMAS and made improvements on it. Furthermore, anonymity was added to the scheme. Even with these improvements, ASMAS was still unable to resist the collusion attacks.

Consider the following scenario:

1) Suppose the adversary can control two legitimate wireless sensor nodes MS1 and MS2 with the same HLR, and that their identities are IDM1 and IDM2, respectively.

2) MS1 and MS2 have each obtained their respective key pairs (e_{IDM1}, s_{IDM1}) and (e_{IDM2}, s_{IDM2}) from their registered HLR.

3) Through the ASMAS scheme, we can know that:

$$s_{IDM1} = \delta_{IDM1} - x \cdot e_{IDM1} = \frac{h(x, IDH)}{h(IDM1, IDH)} - x \cdot e_{IDM1} \bmod q \quad \ldots\ldots (1)$$

$$s_{IDM2} = \delta_{IDM2} - x \cdot e_{IDM2} = \frac{h(x, IDH)}{h(IDM2, IDH)} - x \cdot e_{IDM2} \bmod q \quad \ldots\ldots (2)$$

4)Through equations (1) and (2), we can easily obtain:

$$x = \frac{h(IDM1, IDH)s_{IDM1} - h(IDM2, IDH)s_{IDM2}}{h(IDM2, IDH)e_{IDM2} - h(IDM1, IDH)e_{IDM1}} \bmod q$$

Hence, the private key x of HLR is obtained by the adversary.

4. Comprehensive analysis

After summarizing the above attack methods, we have the following comprehensive analysis:

(1) Security under passive attacks

Passive attacks in WSN environments generally refer to the eavesdropping and interception. As all the data in the WSNs are sent and received through broadcasting, neither managers nor users of WSNs are able to prevent the data in transit from being eavesdropped or intercepted by adversaries. Thus, for this kind of widespread passive attacks, the designers of WSN security system can only try to enhance the confidentiality of data by approaches such as using more secure, efficient algorithms or using more secure channels.

(2) Device security

Device security has always been a research hotspot in the field of WSN security as well. After all, wireless sensor nodes are often distributed in areas beyond the control of administrators, such as areas that are hard to reach by humans or those controlled by adversaries. So, how to ensure the security of these tiny devices has become one of the research topics. As mentioned earlier, wireless sensor nodes can be easily captured or destroyed due to their own nature. Review of existing research shows that most studies focus on privacy protection of data stored on the wireless sensor nodes, such as using better privacy protection schemes, or using more secure hardware.

(3) Non-repudiation

Non-repudiation is one of the security attributes of network information security, which must be considered by designers of WSN security systems. In the early identity authentication schemes, all the participants in the authentication process sent and received messages in their own identities, which basically met the non-repudiation requirements. However, with the diversification of attack means, the security of these schemes has been seriously threatened. Accordingly, some researchers introduced anonymity into the WSN identity authentication schemes to allow the multiple participants of identity authentication to send and receive information in an anonymous way. This greatly enhanced the security of schemes, but ignored the non-repudiation. Man-in-the-middle attacks under some special conditions, collusion attacks and the above-mentioned smart card theft

attacks could all pose serious threats to these anonymous identity authentication schemes, because although the scheme participants can certify the correctness and legitimacy of the information received, they were not necessarily able to authenticate whether the source of these messages is as claimed. Some schemes, in order to enhance efficiency, also employ the hash function to reduce the energy consumption of wireless sensor nodes [27], which makes it more difficult to achieve non-repudiation due to the one-wayness of hash function. At present, all the mainstream schemes achieve anonymity by participating in the authentication using pseudo-identifiers instead of identity. If these pseudo-identifiers are fixed, they will not differ much from the real identities; and if they change frequently, they will offer opportunities to the adversaries, who will implement masquerading attacks taking advantage of the defect in non-repudiation. The general solution now is to authenticate the identities of all participants with pseudo-identifiers via a trusted third party. But this also increases the consumption of WSN resources to some extent.

5. Conclusion

Depending on the hierarchy and structure, WSNs are classified mainly into two types: wireless sensor node–data center WSNs and wireless sensor node–cluster head node–data center WSNs. Security system is one of the important guarantees for normal operation of WSNs, whereas identity authentication scheme is one of the hot research topics in the field of WSN security.

Before designing a WSN-based identity authentication scheme, the security requirements of the WSN and security risks it faces need to be considered carefully. Meanwhile, designers should also have an understanding of the mainstream attack methods against WSNs. After analyzing the security status of WSN-based identity authentication schemes, the risks present in these schemes are obtained: passive attack, device security and non-repudiation. Currently, adversaries launch attacks to WSNs relying mainly on these risks, which are not only the most vulnerable aspects of WSNs, but are also easily ignored by the identity authentication scheme designers. Therefore, in the future design of identity authentication schemes, the above vulnerabilities must be carefully considered.

6. Acknowledgements

This work was financially supported by the Shanghai Natural Science Foundation (0666666), Innovation Program of Shanghai Municipal Education Commission (060000) and Shanghai Leading Academic Discipline Project of Shanghai Municipal Education Commission (0555555).

References

1. Yick J, Mukherjee B, Ghosal D. Wireless sensor network survey[J]. Computer networks, 2008, 52(12): 2292-2330.
2. Kuorilehto M, Hännikäinen M, Hämäläinen T D. A survey of application distribution in wireless sensor networks[J]. EURASIP Journal on Wireless Communications and Networking, 2005, 2005(5): 1-15.
3. Rawat P, Singh K D, Chaouchi H, et al. Wireless sensor networks: a survey on recent developments and potential synergies[J]. The Journal of supercomputing, 2014, 68(1): 1-48.
4. Tubaishat M, Zhuang P, Qi Q, et al. Wireless sensor networks in intelligent transportation systems[J]. Wireless communications and mobile computing, 2009, 9(3): 287-302.
5. Wang Y C, Wu F J, Tseng Y C. Mobility management algorithms and applications for mobile sensor networks[J]. Wireless Communications and Mobile Computing, 2012, 12(1): 7-21.

6. Khalid O, Khan S U, Madani S A, et al. Comparative study of trust and reputation systems for wireless sensor networks[J]. Security and Communication Networks, 2013, 6(6): 669-688.
7. Deif D S, Gadallah Y. Classification of wireless sensor networks deployment techniques[J]. IEEE Communications Surveys & Tutorials, 2014, 16(2): 834-855.
8. Djenouri D, Khelladi L, Badache N. A survey of security issues in mobile ad hoc networks[J]. IEEE communications surveys, 2005, 7(4): 2-28.
9. Zhou Y, Fang Y, Zhang Y. Securing wireless sensor networks: a survey[J]. IEEE Communications Surveys & Tutorials, 2008, 10(3): 6-28.
10. Patel M M, Aggarwal A. Security attacks in wireless sensor networks: A survey[C]//Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on. IEEE, 2013: 329-333.
11. Das A P, Thampi S M. Secure communication in mobile underwater wireless sensor networks[C]//Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on. IEEE, 2015: 2164-2173.
12. Bubinska M, Risteski A. Performance Analysis of Wireless Sensor Networks Under DDoS Attack[C]//Future Access Enablers of Ubiquitous and Intelligent Infrastructures. Springer International Publishing, 2015: 226-232.
13. Buratti C, Conti A, Dardari D, et al. An overview on wireless sensor networks technology and evolution[J]. Sensors, 2009, 9(9): 6869-6896.
14. Khan M K, Alghathbar K. Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks'[J]. Sensors, 2010, 10(3): 2450-2459.
15. Ruiz L B, Nogueira J M, Loureiro A A F. Manna: A management architecture for wireless sensor networks[J]. IEEE communications Magazine, 2003, 41(2): 116-125.
16. Zhang J, Varadharajan V. Wireless sensor network key management survey and taxonomy[J]. Journal of Network and Computer Applications, 2010, 33(2): 63-75.
17. Al Ameen M, Liu J, Kwak K. Security and privacy issues in wireless sensor networks for healthcare applications[J]. Journal of medical systems, 2012, 36(1): 93-101.
18. Butun I, Morgera S D, Sankar R. A survey of intrusion detection systems in wireless sensor networks[J]. IEEE Communications Surveys & Tutorials, 2014, 16(1): 266-282.
19. Turkanovic. M, Brumen. B, Holbl. M, A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion[J]. Ad hoc Networks. 2014(20):96-112
20. P. C. Kocher, J. Jaffe, B. Jun. Differential power analysis[M]. Proceedings of the 19th Annual Interational Crypto;ogy Conference an Advances in Cryptology. Springer-Verlag. 1999:388-397
21. Anand Jose, Sivachandar K. Vampire Attack Detection in Wireless Sensor Network[J]. International Journal of Engineering Science and Innovative Technology (IJESIT). 2014, 3(7):6888-6895
22. Vasserman Eugene Y., Hopper Nicholas. Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks[J]. IEEE Transactions on Mobile Computing. 2013, 12(2):318-332
23. Sun Xin-jiang, Wu Xiao-bei, Huang Cheng, Xu Zhi-liang, Zhong, Jian-lin. Modified access polynomial based self-healing key management schemes with broadcast authentication and enhanced collusion resistance in wireless sensor networks[J]. Ad hoc Networks. 2015(37):324-336
24. Mao Ke-fei, Liu Jian-wei, Chen Jie.Anticollusion Attack Noninteractive Security Hierarchical Key Agreement Scheme in WHMS[J]. Journal of Electrical and Computer Engineering. 2016
25. Tang Cai-mu，Wu Da-peng Oliver. An Efficient Mobile Authentication Scheme for Wireless Networks[J]. IEEE Transactions on Wireless Communications，2008，7（4）：1408-1416.
26. Chang Chin-Chen，Tsai Hao-Chuan. An Anonymous and Self-Verified Mobile Authentication with Authenticated Key Agreement for Large-Scale Wireless Networks[J]. IEEE Transactions on Wireless Communications，2010，9（11）：3346-3353.

27. Chang Chin-Chen, Le Hai-Duong. A Provably Secure, Efficient, and Flexible Authentication Scheme for Ad hoc Wireless Sensor Networks[J]. IEEE Transactions on Wireless Communications. 2015, 15(1):357-366.