Send Orders for Reprints to reprints@benthamscience.ae

944 *The Open Cybernetics & Systemics Journal,* 2014, *8,* 944-950

Open Access

Multi-User Broadcast Authentication Protocol in Wireless Sensor Networks against DoS Attack

Jie Xu[1,2] and Lanjun Dang[3,*]

[1]*School of Electronic Engineering, Xidian University, Yanta District, Xi'an, 710071, China;* [2]*School of Information and Control Engineering, Xi'an University of Architecture and Technology, Yanta District, Xi'an, 710055, China;* [3]*State Key Laboratory of Integrated Service Networks, Xidian University, Yanta District, Xi'an, 710071, China*

Abstract: In order to achieve the multi-user broadcast authentication in WSNs (Wireless Sensor Networks) defending against DoS (Denial-of-Service) attack, a multi-user broadcast authentication protocol in WSNs was proposed based on the improved ECDSA (Elliptic Curve Digital Signature Algorithm) with partial message recovery. The authenticity of the user public key is verified by using bloom filter, which reduces the storage overhead of sensor nodes. The bogus messages are filtered using pre-authentication scheme based on one-way Hash key chain. Theoretical analyses show that, the proposed protocol can resist active attack, compromise attack, and DoS attack. Compared with DDA-MBAS, the proposed protocol reduces the energy consumption of sensor node by about 41.3% while improving the scalability.

Keywords: Broadcast authentication, DoS (Denial-of-Service) attack, hash, WSNs (Wireless Sensor Networks).

1. INTRODUCTION

Wireless sensor networks (WSNs) are the key techniques in Internet of things, and can be widely applied to environmental monitoring, medical care, battlefield surveillance, disaster relief and so on. The open nature of the sensing field and wireless communication make WSNs more susceptible to passive eavesdropping, packet modification, denial-of-service (DoS) attack, node compromise and other security threats. In WSNs, a number of users will join in WSNs and broadcast messages to the networks dynamically to query and collect the latest sensed data. Hence, multi-user broadcast authentication is indispensable for WSNs. In addition, a simple DoS attack can render a large number of resource-constrained sensor nodes crashed (*i.e.*, energy depletion). Therefore, a multi-user broadcast authentication protocol must defend against DoS attack. This paper focuses on multi-user broadcast authentication in WSNs and its strategy of resisting DoS attack, taking the efficiency into account.

Recent works have showed that elliptic curve cryptosystems (ECC) is viable and efficient on resource-limited sensor platforms [1-6]. For example, a 160-bit ECC fixed-point scalar multiplication takes only 0.5 second (s) on an ATmega128L microprocessor at 8MHz [4]. ECC-based broadcast authentication in WSNs becomes a hot research topic because it overcomes the shortcoming of delayed message authentication that is intrinsic to μTESLA-like schemes. However, the WSNs that employ signature-based broadcast authentication protocols are vulnerable to DoS attack. An adversary can easily broadcast a large number of bogus messages to the networks, thus exhausting the energy of sensor nodes within one hop because the sensor nodes must carry out continuous signature verification. Therefore, it is essential that an efficient false message filtering mechanism is added to the signature-based broadcast authentication protocols in WSNs. Nevertheless, most existing multi-user broadcast authentication protocols are unable to filter the false messages with low energy consumption. Currently, the strategies of defending against DoS attack in WSNs are roughly divided into three groups. The schemes in the first group [7, 8] are based on the message-specific puzzles. The major drawback of these schemes is large transmission delay. The second group of solutions [9, 10] filters the false messages using the dynamic window. However, these schemes are only applicable to the static adversaries, and cannot prevent relay attacks. The schemes in the third group [11-14] introduce hash key chain to filter the bogus messages. The schemes [11, 12, 14] are proposed to secure the messages that the sink broadcasts. Since the hash key chains are produced for the sink, the users, and sensor nodes, sensor nodes store too much keys and the scheme [13] has limited scalability. Moreover, the scheme [13] only applies to the static users.

In this paper, we propose a secure and efficient multi-user broadcast authentication protocol in WSNs with resisting DoS attack. There are four major contributions in this paper: (1) The paper proposes a variant of Elliptic Curve Digital Signature Algorithm (ECDSA) with partial message recovery [15], which removes the modular inversion operations of the signature and verification process, for securing the users' broadcast messages in WSNs. (2) The user's ownership over his public key is proven by using bloom filter, which saves the storage space of sensor nodes. (3) Based on one-way hash key chain, an efficient bogus message filtering scheme

1874-110X/14

is proposed to defend against DoS attack. The scheme generates the pre-authentication hash key chains only for the sink and the users, thus having less storage overhead of sensor nodes than the protocol [13]. Therefore, the proposed protocol provides better scalability than the protocol [13]. Moreover, the users are no longer limited to static state in the proposed protocol. (4) The total energy consumption of sensor node can be reduced by about 41.3% because the proposed protocol has shorter broadcast messages and less signature verification, compared with the protocol [13].

The rest of this paper is given as follows. In Section 2, we propose and describe a variant of partial recovery ECDSA. Section 3 proposes a secure and efficient multi-user broadcast authentication protocol in WSNs against DoS attack. Section 4 are the security analyses of the proposed protocol. Quantitative performance analyses are given in Section 5. Section 6 presents the conclusion.

2. A VARIANT OF ECDSA WITH PARTIAL RECOVERY

The ECDSA with partial recovery proposed in [15] is a suitable candidate for WSNs because it only needs two scalar multiplications and one modular inversion in the verification process and partial message is not transmitted over the link. To reduce the computation energy consumption of sensor node, we propose a variant of the scheme in [15], which excludes the modular inversion in the signature and verification process. The variant of ECDSA with partial recovery is described as follows.

Elliptic curve domain parameters: Let elliptic curve domain parameters D=(q, FR, a, b, G, n, h). Let $\boldsymbol{E}/\mathrm{F}_q$ be an elliptic curve over a finite field F_q of characteristic q, *i.e.*, E: $y^2=x^3+ax+b$, where $a,b\in \mathrm{F}_q$, $4a^3+27b^2 \in \mathrm{F}_q^*$, and $q\neq 2, 3$. The points on $\boldsymbol{E}/\mathrm{F}_q$ and a point at infinity $\mathcal{O}$ form the cyclic group G. Suppose that P is a generator of G, whose order is n. One cryptographic hash function is chosen: h: $\{0, 1\}^* \rightarrow Z_n^*$.

Key pair generation: Signer A selects a random integer d in the interval [1, n-1], and computes his public key

$$Q=dP. \tag{1}$$

Then signer A publishes his public key and keeps his private key d secret.

Signature generation: To sign a message $m\in \{0, 1\}^*$ with the domain parameters and his public/private key, the signer A does the following: (1) Chooses a random integer $k\in$ [1, n-1]. (2) Computes $K=kP=(x_1, y_1)$, and $r= x_1 \mathrm{mod} n$. If r equals zero, then go to step (1). (3) Breaks the message m into two parts, *i.e.*, $m=m_1||m_2$, where $|m_1|\leq 10$B. (4) Forms f_1 by adding proper redundancy to m_1 along IEEE P1363a standard. (5) Encode and hash K as an integer i. (6) Computes

$$c=i+ f_1 \mathrm{mod} n. \tag{2}$$

If c=0, then go to step (1). (7) Computes

$$f_2=h(m_2), \tag{3}$$

$$s=k-d(c+f_2)\mathrm{mod}n. \tag{4}$$

If s=0, then go to step (1). Let A's signature over the message m be $\sigma = (c, s)$. Finally, signer A sends (m_2, σ) to a verifier B.

Signature verification: On receiving the partial message m_2 and the signature σ, the verifier B verifies the signature σ and recover the message m with A's public key Q as follows: (1) Discard the message if $c\neq$[1, n-1] or $s\neq$[1, n-1]. (2) Computes $f_2=h(m_2)$. (3) Computes

$$X=sP+(c+f_2)Q=(x_1, y_1). \tag{5}$$

If $X=\mathcal{O}$, the message is discarded. (4) Encode and hash X as an integer i. (6) Computes

$$f_1= c - i \mathrm{mod} n. \tag{6}$$

If the redundancy f_1 of is incorrect, the message is discarded. (7) Recovers m_1 from f_1, and then forms the message m.

The correctness of the signature verification: If (c, s) is A's signature for the message m, then we have $s=k-d(c+f_2)\mathrm{mod}n$. Therefore, the equation $sP+(c+f_2)Q=(s+d(c+f_2))P=kP$ holds.

3. PROPOSED MULTI-USER BROADCAST AUTHENTICATION PROTOCOL WITH RESISTING DOS ATTACKS

The ECDSA with partial recovery proposed in [15] is a suitable candidate for WSNs because it only needs two scalar multiplications and one modular inversion in the verification process and partial message is not transmitted over the link. To reduce the computation energy consumption of sensor node, we propose a variant of the scheme in [15], which excludes the modular inversion in the signature and verification process. The variant of ECDSA with partial recovery is described as follows.

3.1. Design Principle

The proposed protocol should (1) meet the safe condition of broadcast authentication protocol, *i.e.*, no adversary can forge the broadcast data packets correctly; (2) provide the revocation of user to deter compromise attack; (3) defend against DoS attack; (4) achieve good scalability; (5) packet-loss resilience; (6) minimize the energy consumption of sensor node.

3.2. Protocol Description

The proposed protocol is composed of six parts: 1) System initialization. 2) User addition. 3) Message broadcast. 4) Broadcast authentication. 5) User revocation. 6) Key chain update.

3.2.1. System Initialization

There are some assumptions as follows: (1) Elliptic curve domain parameters are preloaded in the users, the sink, and the sensor nodes. (2) The K hash functions are stored in the sink in advance. (3) The sensor nodes are preloaded with the sink's public key. (4) There are L users in WSNs.

First, the sink produces the public keys for all the users, and constructs the set $\mathbf{S}=\{<ID_1,\ Q_{ID_1}>, <ID_2,\ Q_{ID_2}>,\ldots\}$

[16]. The sink uses K hash functions to map the elements of **S** to an m-bit vector $\mathcal{V}=v_0v_1\ldots v_{m-1}$. For $j\in[1, L]$ and $k\in[1, K]$, v_i is set to 1 if $H_k(ID_j||Q_{ID_j})=i$. Otherwise, v_i is set to 0. In order to keep a small probability of a false positive, we have $m<L(2+|Q_{ID}|)$ and $m>KL$, where $|Q_{ID}|$ is the size of Q_{ID}. Then the vector $\mathcal{V}$ is preloaded in each sensor node. For the conveniences of user addition and revocation, the sink also constructs a counting bloom filter to record the number of the set elements that hash to a location.

Each user and the sink respectively select a large random number $k_N^{ID_i} \in F_q$ as the last element to produce their one-way hash key chains of length N by performing hash operation N times, as shown in Fig. (**1**). Namely,

$$k_j^{ID_i} = F(k_{j+1}^{ID_i}),\ 0\le j\le N-1 \tag{7}$$

Here, F is a one-way hash function, *i.e.*, F: $F_q \rightarrow F_q$. Assume that the sensor nodes have stored the identity of each user, the initial keys of one-way hash key chains $k_0^{ID_i}$ and the hash function F.

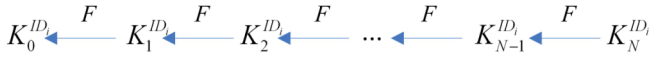

Fig. (1). One-way hash key chain.

3.2.2. User Addition

(1) When a user ID_i joins the networks, the sink generates the key pair (d_{ID_i}, Q_{ID_i}) for the user and updates the counting bloom filter. The increment of vector $\mathcal{V}$ is computed and broadcast to each sensor node by the sink. On receiving the message, a sensor node verifies the signature of the message. If the verification of signature is successful, the sensor node updates the local vector $\mathcal{V}$. (2) The user produces his hash key chain and sends the initial key to the sink. Then the sink broadcasts the identity of the user and the initial key of the hash key chain to the WSNs. The sensor node saves the user's identity and the initial key of key chain if the authentication is passed.

3.2.3. Message Broadcast

When the user ID_i broadcast the first j message $m_j^{ID_i}$, the user first signs the message $M=(m_j^{ID_i}, ID_i, k_j^{ID_i}, tt_j^{ID_i})=M_1||M_2$, where $|M_1|\le 10B$ and $tt_j^{ID_i}$ is the time to send the message, according to the signature stage of the proposed variant of partial recovery ECDSA. Then the user broadcasts the message $<M_2, \sigma_{ID_i}, Q_{ID_i}>$ to the networks, where $\sigma_{ID_i}=(c, s)$ is the user's signature over the message M.

3.2.4. Broadcast Authentication

Upon receiving the broadcast message, a sensor node does the following operations: (1) Checks if the message has ever been received. (2) Judges the freshness of $tt_j^{ID_i}$ by examining whether $\overline{tt} - tt_j^{ID_i} \le \delta$, where $\overline{tt}$ is current time and δ is the predefined time limit of message propagation. (3) Looks up the user's identity in the revocation list. (4) Proves the user's ownership of his public key by checking whether

$$\mathcal{V}[H_k(ID_i||Q_{ID_i})]=1, \text{ where } k\in[1, K] \tag{8}$$

(5) Filters the bogus messages by validating whether the equation $k_r^{ID_i} = F^{j-r}(k_j^{ID_i})$ holds, where $0<j-r<T$ and T is the predefined pocket loss toleration threshold and $k_r^{ID_i}$ is the current pre-authentication key stored in the sensor node. (6) Overlay $k_r^{ID_i}$ with $k_j^{ID_i}$, which is used to filter the coming message. (7) Verify the signature of the message according to the verification part of the proposed variant of partial recovery ECDSA. If the signature verification successes, the sensor node forwards the message to its neighbor nodes. Otherwise, the message is ignored.

Fig. (**2**) illustrates the message broadcast and authentication process.

3.2.5. User Revocation

If a user is compromised by an adversary, or the user wants to leave the networks, the sink will modify the counting bloom filter and broadcast the message containing the user's identity to revoke the user. Once a sensor node receives the message, it will add the identity of the user to its local revocation list. In addition, the sink needs to compute the increment of the vector $\mathcal{V}$ and broadcast it to the networks. Having received the increment of the vector, a sensor node will update the local vector $\mathcal{V}$.

3.2.6. Key Chain Update

When a user's key chain is used up, the user reselects a random large number $k_N^{ID_i} \in F_q$ as the last key of a new key chain. Then the user generates its new one-way hash key chain of length N according to Equation (7). Afterwards, the user broadcasts the new initial key to the networks. Upon receiving the message, a sensor node will replace the key for the false message filtering with the new initial key if the pre-authentication and authentication of the message succeed.

4. SECURITY ANALYSES

4.1. Active Attack

Firstly, the integrity of the broadcast message is ensured in the proposed protocol. When a user needs to broadcast a message $M=(m_j^{ID_i}, ID_i, k_j^{ID_i}, tt_j^{ID_i})=M_1||M_2$, the user first signs the message according to the variant of the partial recovery ECDSA described in Section 2. The hash value of M_2 is computed, as Equation (3), for generating the signature of the message M. Afterwards, only the second part M_2 and signature of the message M are transmitted over links. If an

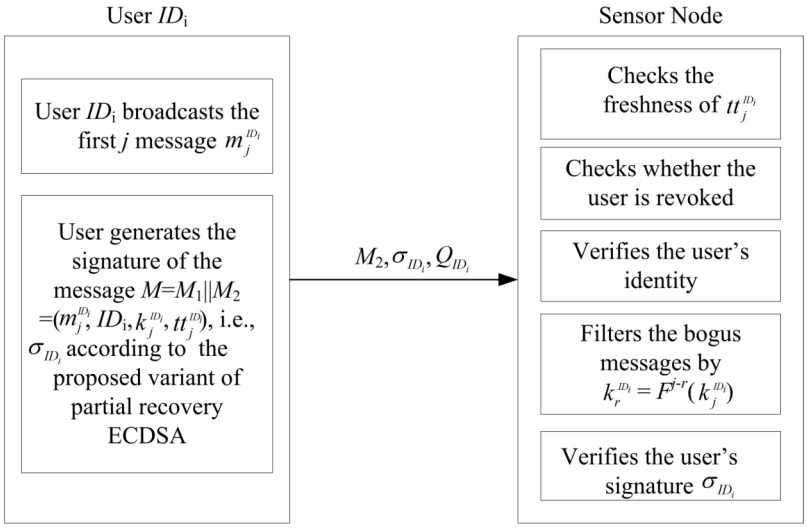

Fig. (2). The message broadcast and authentication process.

adversary modifies M_2 or the signature, the signature is verified unsuccessfully. Therefore, this kind of adversary cannot fool a sensor node.

Secondly, the proposed protocol can achieve source authentication. If an adversary injects a bogus message into the WSNs, the adversary cannot generate the valid signature of the message for the adversary does not know a user's private key. Therefore, a sensor node will drop the message. Even if an adversary knows a user's public key, the user's private key cannot be derived from Equation (1). To compute a user's private key from his public key is as hard as to solve the Elliptic Curve Discrete Logarithm Problem (ECDLP). As a result, the valid signature cannot be generated by the adversary.

Thirdly, the proposed protocol can deter against replay attack by adding a timestamp $tt_j^{ID_i}$ to a broadcast message. Once an adversary broadcasts a message from a previous session, a sensor node will discard the message for the timestamp that is involved in the message is not fresh. Therefore, the replay attack can be defeated in the proposed protocol.

From the three aspects above, we can conclude that the proposed protocol can resist active attack.

4.2. Compromise Attack

By using user revocation scheme, the proposed protocol can thwart the compromise attack. When a user is compromised by an adversary, the adversary can obtain the user's private key. If the adversary impersonates the user to broadcast illegal or junk messages to the WSNs, some sensor nodes will report the abnormal phenomena to the sink. Then the sink broadcasts the compromised user's identity to the networks. After receiving the revocation message, a sensor node will include the compromised user's identity in the local revocation list. Therefore, a sensor node will ignore the messages that are signed by the revoked user's private key. If a sensor node is compromised by an adversary, the users' public keys are accessed by the adversary. The adversary cannot get the users' private key from their public key unless the ECDLP can be solved. As a result, the adversary will not cause damage to the networks.

4.3. DoS Attack

Employing the broadcast authentication based on signature, the proposed protocol can achieve immediate authentication. Therefore, the proposed protocol can resist DoS attack caused by authentication delay. In addition, a typical DoS attack means that adversaries inject a large number of false messages to the networks in order to exhaust the energy and memory of the sensor nodes within one hop. The proposed protocol can defeat this kind of DoS attack by using pre-authentication scheme based on one-way hash key chain. Large numbers of false messages can be filtered by a sensor node with low energy consumption. The pre-authentication process will not cause the long message queue waiting for authentication because hash operation has very low computational complexity. Therefore, the energy and memory of sensor node will not be exhausted in a short time. Therefore, the proposed protocol can reject DoS attack.

5. PERFORMANCE ANALYSES

We compare the performance of the proposed protocol with the existing multi-user broadcast authentication protocol against DoS attack (*i.e.*, DDA-MBAS [13]) in terms of scalability and the energy consumption.

5.1. Scalability

In the proposed protocol, the user can join the networks at any time, or be revoked because of misbehaving and leaving the networks. For example, the MICA2 has 4KB EEPROM, 128KB flash memory of program and 512KB flash memory of measurement. The proposed protocol can support 20*1024/(20+2)=930 users if a memory space of 20KB is used for storing the users' identity and pre-authentication key. Although more memory means more users, in fact, the number of user can not be too much. Otherwise, it can cause serious channel competition and even the communication block [13]. Compared with DDA-MBAS

Table 1. Energy consumption of two compared broadcast authentication protocols.

	Communication Overhead	Communication Energy Consumption	Computing Time	Computation Energy Consumption	Total Energy Consumption
DDA-MBAS	191 bytes	6.45+2.39*N* mJ	2.66 s	63.84 mJ	70.29+2.39*N* mJ
Our protocol	125 bytes	4.22+1.56*N* mJ	1.41 s	33.84 mJ	38.06+1.56*N* mJ

[13], the proposed protocol generates one-way hash key chains only for the sink and each user, thereby saving the storage space of the sensor node. Therefore, the proposed protocol can support more users and thus provide better scalability than DDA-MBAS [13]. In addition, the users are not limited to static state.

5.2. Energy Consumption

Suppose that the sensor node in the WSNs is MICA2. The power level of the node is 3.0 V, the draw in active mode is 8.0 mA, the transmitting draw is 27mA, the receiving draw is 10 mA, and the data rate is 19.2kbps [17]. MICA2 mote uses IEEE 802.15.4 standard. Therefore, one packet transmitted in the physical layer is up to 133 bytes, including a packet header of 31 bytes [18]. We assume that the size of original message is 20 bytes, the size of timestamp is 2 bytes, and the size of ID_i is 2 bytes. The security strength of 1024-bit RSA is as same as 160-bit ECC. One ECC arbitrary point scalar multiplication requires 1.25s on MICA2 mote, and the operation time of one ECC double scalar multiplication is 1.41s [4].

In the proposed protocol, the size of broadcast message is 34+40+20=94 bytes. A MICA2 mote only needs to transmit one packet of 125 bytes in the physical. Therefore, the energy consumptions of transmitting and receiving one broadcast message are $3.0\times27\times10^{-3}\times125\times8/19{,}200=4.22$ mJ and $3.0\times10\times10^{-3}\times125\times8/19{,}200=1.56$ mJ, respectively. Assuming that N is the neighbor density, the communication energy consumption of a sensor node is 4.22+1.56N mJ. If hash operation is ignored, the signature verification requires one ECC double scalar multiplication. Then the computation energy consumption of one sensor node is $3.0\times8\times10^{-3}\times1.41=33.84$ mJ. As a result, the total energy consumption of one sensor node is 38.06+1.56N mJ.

In DDA-MBAS [13], the broadcast message is $< ID_A, i_A, k_A^{i_A}, M, tt, \sigma >$. Then the size of broadcast message is 129 bytes. Hence, two 802.15.4 packets (*i.e.*, 102+31+27+31 = 191 bytes) need to be transmitted by a MICA2 mote in the physical layer. The costs of transmitting and receiving one broadcast message are $3.0\times27\times10^{-3}\times191\times8/19{,}200=6.45$ mJ and $3.0\times10\times10^{-3}\times191\times8/19{,}200=2.39$ mJ, respectively. The communication energy consumption of one sensor node is 6.45+2.39N mJ. In DDA-MBAS, the main operations in verification process are one ECC arbitrary point scalar multiplication and one ECC double scalar multiplication. The computation energy is $3.0\times8\times10^{-3}\times(1.25+1.41)=63.84$ mJ. Therefore, the total energy consumption of one sensor node is 70.29+2.39N mJ in DDA-MBAS [13]. Table **1** lists the comparison result of these two protocols in terms of communication overhead, communication energy consumption, computing time, computation energy consumption, and the total energy consumption.

Fig. (**3**) illustrates the communication energy consumptions of these two protocols. The larger neighborhood den-

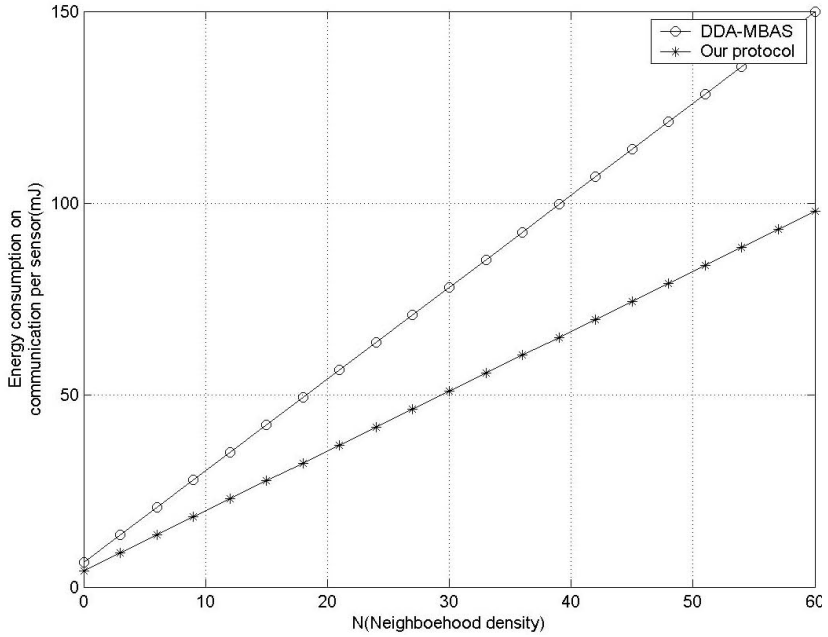

Fig. (3). Comparison of these two protocols on communication energy consumption.

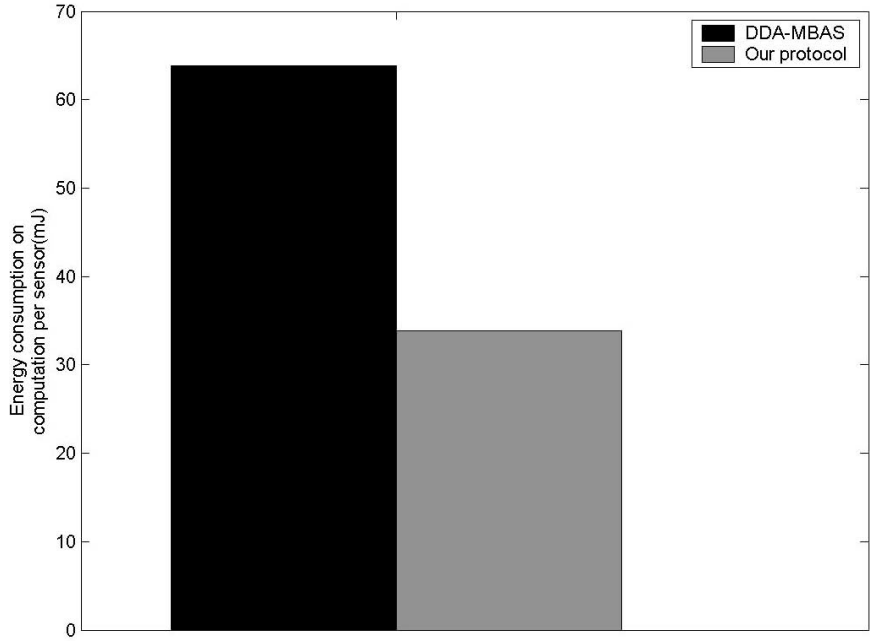

Fig. (4). Comparison of these two protocols on computation energy consumption.

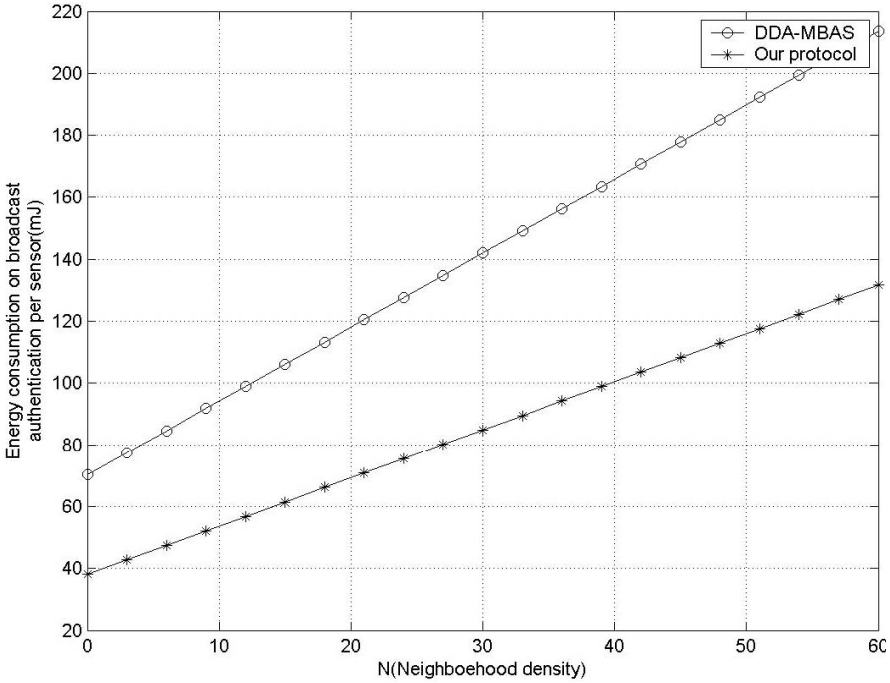

Fig. (5). Comparison of two protocols on total energy consumption.

sity N becomes, the more the communication energy consumption of the proposed protocol is reduced compared to DDA-MBAS. The reasons are (1) the proposed protocol has less communication overhead than DDA-MBAS; (2) one sensor node retransmits once and receives the same message N times.

The computation energy consumptions of these two protocols are shown in Fig. (**4**). From the figure, we can observe that the computation energy consumption of the proposed protocol is less than that of DDA-MBAS. This is because the proposed protocol avoids one ECC arbitrary point scalar multiplication in the signature verification, compared with DDA-MBAS.

Fig. (**5**) shows the relationships between the energy consumption of one sensor node and the neighbor density N in two compared protocols. There is a growing difference of energy consumption between DDA-MBAS and the proposed protocol as neighborhood density N becomes large. Compared with DDA-MBAS [13], the proposed protocol reduces the total energy consumption by 48.73 mJ or 41.3% when neighborhood density N is 20. There are two reasons as follows: (1) the communication overhead in the proposed pro-

tocol is less than that in DDA-MBAS; (2) compared with DDA-MBAS, the proposed protocol has less commuting time in the signature verification.

As a result, the proposed protocol is more efficient that DDA-MBAS [13] in terms of scalability and energy consumption, while providing the same security level.

CONCLUSION

This paper achieves the multi-user broadcast authentication in WSNs by utilizing the proposed variant of ECDSA with partial recovery, and employs bloom filter to authenticate the users' public key in order to save the storage space of a sensor node. The pre-authentication scheme based on one-way hash key chain is designed to filter the bogus message effectively in this paper. A threshold is predefined to tolerate pocket loss. Theoretical analyses demonstrate that, the proposed protocol can defeat active attacks, compromise attacks, and DoS attacks. Particularly, the energy reduction of the proposed protocol achieves 48.73 mJ or 41.3% Compared with DDA-MBAS.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

This work is support by the National Natural Science Foundation of China (NSFC) Grant 61402351, "the Fundamental Research Funds for the Central Universities" JB140116, and the Natural Science Research Project of Education Department of Shaanxi Province of China 12JK0555.

REFERENCES

[1] Faye Y, Guyennet H, Niang I, *et al.*, "Fast scalar multiplication on elliptic curve cryptography in selected intervals suitable for wireless sensor networks," *Cyberspace Safety and Security: LNCS 8300*, Berlin: Springer-Verlag, pp. 171-182, 2013.

[2] Wenger E, "Hardware architectures for MSP430-based wireless sensor nodes performing elliptic curve cryptography," *Applied Cryptography and Network Security: LNCS 7954*, Berlin: Springer, pp. 290-306, 2013.

[3] Faye Y, Guyennet H, Niang I, *et al.*, "Fast Scalar Multiplication on Elliptic Curve Cryptography in Selected Intervals Suitable for Wireless Sensor Networks," *Cyberspace Safety and Security: LNCS 8300*, Berlin: Springer-Verlag, pp. 171-182, 2013.

[4] Liu Z, Seo H, Großschädl J, *et al.*, "Efficient implementation of NIST-compliant elliptic curve cryptography for sensor nodes," *Information and Communications Security: LNCS 8233*, Berlin: Springer-Verlag, pp. 302-317, 2013.

[5] Liu Z, Wenger E and Großschädl J, "MoTE-ECC: Energy-scalable elliptic curve cryptography for wireless sensor networks," *Applied Cryptography and Network Security: LNCS 8479*, Berlin: Springer-Verlag, pp. 361-379, 2014.

[6] Indra G and Taneja R, "A time stamp–based elliptic curve cryptosystem for wireless ad-hoc sensor networks," *International Journal of Space-Based and Situated Computing*, vol. 4, no.1, pp. 39-54, 2014.

[7] Ning P, Liu A and Du W, "Mitigating DoS attacks against broadcast authentication in wireless sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 4, no.1, pp. 1, 2008.

[8] Jiawei Chen, "Broadcast Authentication Protocol Scheme Based on DBP-MSP and Safe Routing in WSN against DDoS Attacks," *ICNDC 2011*, Piscataway, NJ: IEEE, pp. 170-174, 2011.

[9] Yao L, Yu Z, Zhang T, *et al.*, "Dynamic Window Based Multihop Authentication for WSN," *Proceedings of the 17th ACM Conference on Computer and Communications Security*, New York: ACM, pp. 744-746, 2010.

[10] Xiong K, Wang R, Du W, *et al.*, "Containing bogus packet insertion attacks for broadcast authentication in sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol.8, no. 3, pp. 20, 2012.

[11] Dong Q, Liu D, Ning P, "Pre-authentication filters: providing dos resistance for signature-based broadcast authentication in sensor networks," *Proceedings of the first ACM conference on Wireless network security*, New York: ACM, pp. 2-12, 2008.

[12] Son J H, Luo H and Seo S W, "Denial of service attack-resistant flooding authentication in wireless sensor networks," *Computer Communications*, vol. 33, no. 13, pp. 1531-1542, 2010.

[13] Jianghong Guo and Jianfeng Ma, "Multi-user broadcast authentication scheme in wireless sensor networks with defending against DoS attacks," *Journal on Communications*, vol. 32, no. 4, pp. 94-102, 2011. *(in Chinese)*

[14] Dong Q, Liu D and Ning P, "Providing DoS resistance for signature-based broadcast authentication in sensor networks," *ACM Transactions on Embedded Computing Systems (TECS)*, vol.12, no.3, pp. 73, 2013.

[15] D. Naccache, J. Stern, "Signing on a postcard," *Financial Cryptography: LNCS 1962*, Berlin: Springer, pp. 121-135, 2001.

[16] K. Ren, S. Yu, W. Lou, *et al.*, "Multi-user broadcast authentication in wireless sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 8, pp. 4554-4564, 2009.

[17] Crossbow technology, "*MICA2 datasheet*," Sept. 2014. [Online] Available from: http://www.investigacion.frc.utn.edu.ar/senso--res/Equipamiento/Wireless/MICA2_Datasheet.pdf.

[18] IEEE P802.15 Working Group. IEEE Std 802.15.4, IEEE standard for information technology – telecommunications and information exchange between systems – local and metropolitan area networks, part 15.4: wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs). New York: IEEE, 2006.

[19] IEEE P802.15 Working Group. IEEE Std 802.15.4, IEEE standard for information technology – telecommunications and information exchange between systems – local and metropolitan area networks, part 15.4: wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs). New York: IEEE, 2006.

Received: September 16, 2014 Revised: December 23, 2014 Accepted: December 31, 2014