doi:10.3772/j.issn.1006-6748.2018.03.009

OvBNN authentication based on cooperative signature for wireless sensor networks[①]

Qin Danyang (秦丹阳)[②], Zhang Yan, Ma Jingya, Ji Ping
(Key Lab of Electronic and Communication Engineering, Heilongjiang University, Harbin 150080, P. R. China)

Abstract

The universality of the application of wireless sensor networks (WSN) makes more attention be paid on the security problem. Node authentication is not only the basis of network security, but also the premise of key management and secure routing protocol. Although the signature mechanism based on symmetric encryption is high in energy efficiency, it is vulnerable to be attacked and there is a time delay during authentication. Traditional public key encryption mechanism with improvement in security brings in complex algorithm and costs much time, which is not suitable for WSN. In this paper, a signature authentication mechanism, an optimized variant Bellare Namprempre Neven (OvBNN) is presented to quickly complete the authentication by mutual cooperation between nodes so as to make the nodes use the intermediate calculation results of their neighbor nodes directly. Simulation results show that the proposed mechanism is superior to traditional authentication mechanisms both in energy consumption and authentication time.

Key words: optimized variant Bellare Namprempre Neven (OvBNN), digital signature, authentication speed, energy consumption, wireless sensor networks (WSN)

0 Introduction

Wireless sensor network (WSN) is a multi-hop mobile network deployed in hostile or unmanned areas, which is composed of a great number of nodes in a self-organized manner[1]. Due to the features including fast deployment, low cost, fault tolerance and so on, WSN has been widely used in a lot of aspects, such as military, national defense, field inspection, environmental monitoring, disaster prevention and other fields. Although the wireless sensor network has a wide range of applications, it also has many limiting factors, such as limited power supply, limited storage capacity and limited communication capacity[2]. In the condition of various restrictions, how to make the operation of network security will undoubtedly become an important part which can't be ignored. As the core and important basic link of the security mechanism, how to complete the authentication safely, efficiently and in low- energy is always a research hot spot in wireless sensor network.

μTESLA is a time-based high-efficient and tolerating of packet dropout symmetric key encryption protocol. The protocol is based on the TESLA authentication protocol, which improves the key update process and initial authentication process, and solves the unidirectional problem of the key generation algorithm and the problem of key distribution packet loss[3] in order to make the network effectively implemented. But it is vulnerable to denial of service (DoS) attacks, so that the network can't provide normal services. The public key encryption mechanism is different from symmetric encryption, and both communication sides do not need to have a common key[4]. Even if the public key is acquired by an attacker during the delivery or release process, the attacker will not obtain any useful information for the private key is not matched with the public key[5]. Since WSN has resource-constrained features, the authentication mechanism should have characteristics of energy saving and high operation speed. But the public key encryption algorithm is complex, and running velocity is relatively slow. Ref. [6] presented a fast signature authentication mechanism to improve the authentication efficiency, but the energy consumption is too high for wireless sensor networks. On this basis, this paper takes into account both the ener-

[①] Support by the National High Technology Research and Development Program of China (2012AA120802), the National Natural Science Foundation of China (61771186), the Postdoctoral Research Project of Heilongjiang Province (LBH-Q15121) and the Undergraduate University Project of Young Scientist Creative Talent of Heilongjiang Province (UNPYSCT-2017125).

[②] To whom correspondence should be addressed. E-mail: qindanyang@hlju.edu.cn

Received on Nov. 9, 2017

gy cost and security performance and proposes a new signature authentication mechanism based on the variant Bellare Namprempre Neven (vBNN), by saving node energy and improving the authentication speed to prolong the network life effectively.

1 vBNN scheme

1.1 Elliptic curves cryptography

Victor Miller and Heal Kablitz first proposed the elliptic curves cryptography (ECC) in 1985. The increasement of security demand in recent years makes ECC become an effective selection for researchers. The security of elliptic curves cryptography is based on the difficulty of the problem of the elliptic curve discrete logarithm. Its high-level security brings many advantages: the shorter key length, the smaller digital signature and the faster operation speed. Table 1 represents the key size required for ECC and RSA (Rivest Shamir Adleman) at the same deciphering time.

Table 1 Key size of ECC and RSA with the same deciphering time

Decode time (MIPS)	Key length of ECC	Key length of RSA	Ratio
10^4	106	512	1:5
10^8	132	768	1:6
10^{12}	160	1024	1:7
10^{20}	210	2048	1:10

The elliptical curve is defined by a binary cubic equation, the elliptic curve's representation on different number field is different, even the operation on it is not the same. There are two types of elliptical curves, elliptical curves on the finite field GF(p) and GF(2^m) are most commonly used[7]. Assuming that there is $p > 3$, an elliptic curve on the finite field Z_p can be defined as

$$E/Z_p:\ y^2(\bmod\ p) = x^3 + ax + b \tag{1}$$

where $a,\ b \in Z_p$, $4a^3 + 27b^3 \neq 0(\bmod p)$.

Supposing that P is the point in field Z_p, in which the P' s order is p. G is the group produced by the "add" operation of the point. Two points M and N are taken on the elliptical curve E, where l is the straight line linking point M and N, and intersects elliptic curve at point R. The addition of the elliptic curve on the finite field is as follows: assuming there is $M = (x_1,\ y_1)$ and point $N = (x_2,\ y_2)$, $M,\ N \in E(a,b)$, the addition operation will satisfy:

$$M + N = \begin{cases} O, & x_1 = x_2,\ y_1 = -y_2 \\ (x_3,\ y_3), & \text{others} \end{cases} \tag{2}$$

where, there are $x_3 = \lambda^2 - x_1 - x_2(\bmod p)$, and $y_3 = \lambda(x_1 - x_3) - y_1(\bmod p)$. For $M \neq N$, there will be $\lambda(\bmod p) = (y_2 - y_1)/(x_2 - x_1)$. There are two points M and N on the ECC and which x axis is different, then $M + N = -R$[8]. The multipoint operation on ECC is defined as $tP = P + P + \cdots + P$, the number of point P is t. The elliptic curve discrete logarithm problem (ECDLP) is the problem of getting t given $tP$and P.

1.2 Realization process of vBNN

vBNN signature mechanism is an improved BNN-IBS (Bellare Namprempre Neven identity-based signature) signature mechanism[9], and it is an ECC-based encryption method. In wireless sensor networks, because the BNN-IBS's data packet size is large, vBNN scheme reduces the packet size on the basis of vBNN effectively. The implementation steps of vBNN are as follows:

1) Preliminary: The private key generator (PKG) is a credible third party, which can generate private key P_{ria} for users. The public key is the user's identity or other public information. Given the safety parameters k, PKG will take the following steps.

Ⅰ. Define elliptic curve E over field Z_p and point P with order p;

Ⅱ. Select private key randomly in Z_p, and calculate P_0 by $P_0 = xP$ as the system public key;

Ⅲ. Define Hash functions as $\mathrm{H}_1:\ \{0,1\} \times G_1^* \rightarrow Z_p$ and $\mathrm{H}_2:\ \{0,1\}^* \rightarrow Z_p$;

Ⅳ. Obtain parameters $(E/Z_p,\ P,\ p,\ P_0,\ H_1,\ H_2)$, where x is unknown.

2) Keys extraction: $ID_a \in \{0,1\}^*$ is the unique identity for user A, and different users will have different identities;

Ⅰ. Select random number r from Z_p to calculate R by $R = rP$;

Ⅱ. Calculate $c = \mathrm{H}_1(ID_a \| R)$ and $s = r + cx$.

In this stage, $P_{ria} = (R,\ s)$ is the private key for user A.

3) Generate signature: Assuming the identity of user A is ID_a, A is the node who carries message m.

Ⅰ. Select random number y from Z_p to calculate Y by $Y = yP$.

Ⅱ. Calculate $h = H_2(ID_a,\ m,\ R,\ Y)$ and $z = y + hs$.

In this stage, $(R,\ h,\ z)$ is the signature of user A.

4) Signature verification:

Ⅰ. Calculate $c = \mathrm{H}_1(ID_\mathrm{a} \| R)$;

Ⅱ. Verify whether obtained parameter h is valid by $h = \mathrm{H}_2(ID_\mathrm{a}, \mathrm{m}, R,\ zP - h(R + cP_0))$;

Ⅲ. The signature verification is completed if the equation in step b is valid, or else the system will reject the signature to set it as invalid.

2 Network model and attack model

The network model and attack model for the proposed mechanism will be described in this section.

2.1 Network model

It is supposed that WSN satisfies the characteristics of large scale, static and high node deployment density. As the sensor node is active, it couldn't be charged in low power, so the nodes in WSN transfer the data from the source node to sink node by the way of multi-hop. Each sensor node is deployed in a fixed position or moving very slowly. Similar networks can also be deployed in environmental monitoring and smart home applications. Through analysis and process to the data collected from the sensor nodes, people can get necessary information timely.

2.2 Attack model

Wireless sensor networks are vulnerable to multiple attacks due to the special nature of wireless transmission. An attacker could capture some sensor nodes or transmit bogus information to the network, reducing the reliability of information that the user gets. WSN may suffer the following attacks.

(1) Exhaustion attack: If loopholes exist in the wireless sensor protocol, an attacker may keep sending useless data packets to one sensor node. Then legitimate users will not be able to access to this node, because limited energy will be cost by such useless data packets. The incidence of the exhaustion attacks can be alleviated if the network can control the number of nodes sending data packets.

(2) DoS attack: Once sensor nodes are captured by the attacker, the nodes will send high priority packets to other nodes. These packets will occupy the transmission channel, so the legitimate data packets can't be transmitted timely, resulting in the whole network denial of service. This type of attack may exist in the four lower layers of OSI network model. Reducing the priority difference of different data packets can reduce the damage to the network caused by DoS attack.

(3) Flooding attack: Malicious nodes under this attack often have sufficient charge, and they will broadcast Hello message to the legitimate node. Receiving such Hello message, the node may think the malicious one is its neighbor and will send the information to the malicious node, but actually these nodes may be too far from each other to complete the data packets transmission by one hop.

(4) Wormhole attack: The malicious node under the attack usually has a strong ability to send and receive data packets, while the legal node will take the malicious node mistakenly for the relay message in the process of multi-hop transmission, making the two multi-hop nodes think the routing path of them are single-hop, so as to destroy the routing structure of the network.

3 Optimized vBNN signature scheme

In this section, general idea of the OvBNN signature mechanism will be presented and the authentication process will be established.

The vBNN signature authentication mechanism is discussed in detail in the second part. Each sensor node needs to calculate zP-hR-hcP_0 to complete the authentication, but the nodes should first calculate the value of zP, hR and hcP_0 to obtain the final sum. The repeated calculating operations by each sensor will undoubtedly slow down the authentication efficiency of the node as well as shorten the network life. In OvBNN proposed in this paper, if a node is willing to consume its own energy to transmit one or all of its calculated intermediate results to its neighbor nodes, the neighbor node will reduce the calculation procedure so as to speed up the authentication.

Assume that a packet $\{m,\ ID_u,\ pt,\ Sig_m\}$ is broadcasted by the user, where m represents the useful infor*m*ation, ID_u is the user's unique identity, pt is the present time of sending the packet, and Sig_m is the user's signature for m. When a node receives a packet to send to the next hop, the first step is to check whether the packet is out of date.

OvBNN authentication process is shown in Fig. 1. In this figure, a user is going to send packets to three neighbor nodes, namely A, B and C. They are willing to transmit one of the intermediate calculation results zP, hR and hcP_0 to their neighbor nodes after being verified. Suppose that node A, B and C will send zP, hR and hcP_0 respectively. Since node E will receive intermediate result zP from node A, it can complete the authentication after adding the value of hR and hcP_0. Compared to the traditional vBNN, OvBNN only needs two multiplications and two additions to complete the authentication by reducing one multiplication during the process. Similarly, node F and node I will receive hR and hcP_0 of node B and node C respectively, and perform twice multiplications and twice additions to complete the authentication. Since nodes D, G, and H are also the neighbor nodes of nodes A, B and C, respectively, the authentication modes are the same as the nodes C, F, and I. Similarly, nodes D, F, and H can continue to transfer their intermediate results to other neighbor nodes that have to be authenticated. In traditional vBNN mechanism, each node needs 3mul + 2add to complete the authentication, while OvBNN proposed in this paper requires only 2mul + 2add.

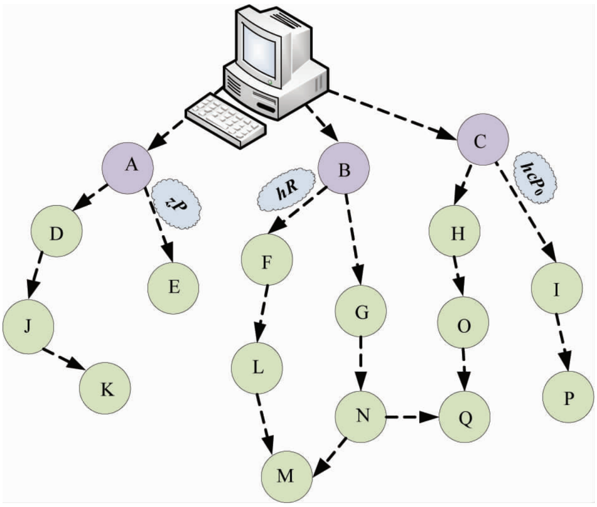

Fig. 1 OvBNN authentication by cooperation among nodes

Moreover, OvBNN can save more energy if the node sends some of its intermediate calculation results directly to the neighbor. The procedure above only pass one of the factors as zP, hR and hcP_0. Now, the condition that the node will transmit the value of $zP-hR$、$hR + hcP_0$ or $zP + hcP_0$ will be discussed. Taking node C as an example, which is willing to consume part of its energy to deliver the intermediate calculation results $hR + hcP_0$ to its neighbor nodes I and H, which only need to calculate their value of zP after receiving $hR + hcP_0$, and add all results together to complete the certification. The entire certification process requires 1mul + 1add by reducing times of calculations to speed up the authentication.

All these three intermediate results being sent to the neighbors will make the network vulnerable to the following attacks. Table 2 and Table 3 show the actions performed by the attackers and the victims.

Table 2 Operations of the attackers

Attacking behaviors
1. To generate a false message m';
2. To choose R', z', h', hc' randomly;
3. To calculate $z'P - h'R' - hc'P_0$;
4. To calculate $h' = H_2(ID_a, m', R', z'P - h'R' - hc'P_0)$;
5. To transmit (R', h', z') and $z'P$, $h'R'$ and $hc'P_0$.

Table 3 Operations of the victims

Victim behaviors
1. To calculate $c' = H_1(ID_a \| \| R')$;
2. To count $H_2(ID_a, m', R', z'P - h'R' - hc'P_0)$;
3. To compare the result from step 2 with h';
4. If consistent, m' will be regarded as effective information.

To make the node authentication efficiency higher, it is assumed that the sensor node only sends the intermediate result $hR + hcP_0$ to its neighbor or the node is unwilling to transmit any calculation results to its neighbors. As shown in Fig. 1, based on the above two assumptions, node C may send the following message packet to its neighbor H: $\{m, ID_u, pt, Sig_m, hR + hcP_0\}$ or $\{m, ID_u, pt, Sig_m\}$. Of course, the intermediate calculation results may also be zP, hR, hcP_0 or the sum result. If the packet $\{m, ID_u, pt, Sig_m\}$ is received by node H, then it will wait for the time of W_t period to see if it will receive the intermediate result from node C (here the intermediate result refers to $hR + hcP_0$). At the same time, node H and I will cache the data packets from node C, the number of data packets is τ. If the node does not receive any intermediate results after W_t, it will perform the calculating operations by 3mul + 2add as the traditional vBNN to complete their own certification. If so, OvBNN will devolve into traditional vBNN.

In the proposed OvBNN signature authentication mechanism, it is assumed that a node has α neighbor nodes, where $\alpha/2$ nodes can receive data packets; there are β nodes to be captured, and each node will generate γ false packets. The number of packets τ will satisfy the following condition as

$$1 + \beta \cdot \gamma \leqslant \tau \leqslant \alpha/2 \tag{3}$$

Waiting time W_t is determined by the value of n, transmission rate $r_{\max}$, packet size S_{pac}, initial backoff $INI_{\max}$, and congestion backoff $CON_{\max}$. Then there will be

$$(INI_{\max} + CON_{\max} + S_{\text{pac}}/r_{\max}) \cdot \tau \geqslant W_t \tag{4}$$

Obviously, the more intermediate results are being transferred, the higher computational efficiency and the more energy consumption there will be. So parameter P_{rel} needs to be set carefully to keep the balance between energy and efficiency. P_{rel} is the probability of the nodes that are willing to transfer the intermediate result to their neighbor nodes. To some extent, the transmission of intermediate results requires energy consumption there will be. The speed of signature verification, however, will be affected if the value of P_{rel} is too low. Once the wireless sensor network is deployed, P_{rel} should be determined according to the topology and dynamic changes of the network to tradeoff the energy cost and certification efficiency. Assuming that there are N nodes in each transmission to have to complete the signature authentication and P_T represents the probability of T nodes transmitting the intermediate calculation results to their neighbor nodes, the relationship between P_T and P_{rel} should satisfy following expression as

$$P_T = \binom{N}{T} \cdot P_{\mathrm{rel}}^{\mathrm{T}} \cdot (1 - P_{\mathrm{rel}})^{(N-T)} \qquad (5)$$

In order to prevent the whole network from being attacked, the node will judge whether message m, signature Sig_m, and $hR + hcP_0$ in the received packet are consistent after waiting time α_t. If they are inconsistent, these packets are discarded and reported to the base station. It is judged whether the packet $\{m, ID, pt, Sig_m, hR + hcP_0\}$ is received if they are consistent. The detailed authentication process of OvBNN is shown in Fig. 2, and the redundancy of the packets will be effectively reduced.

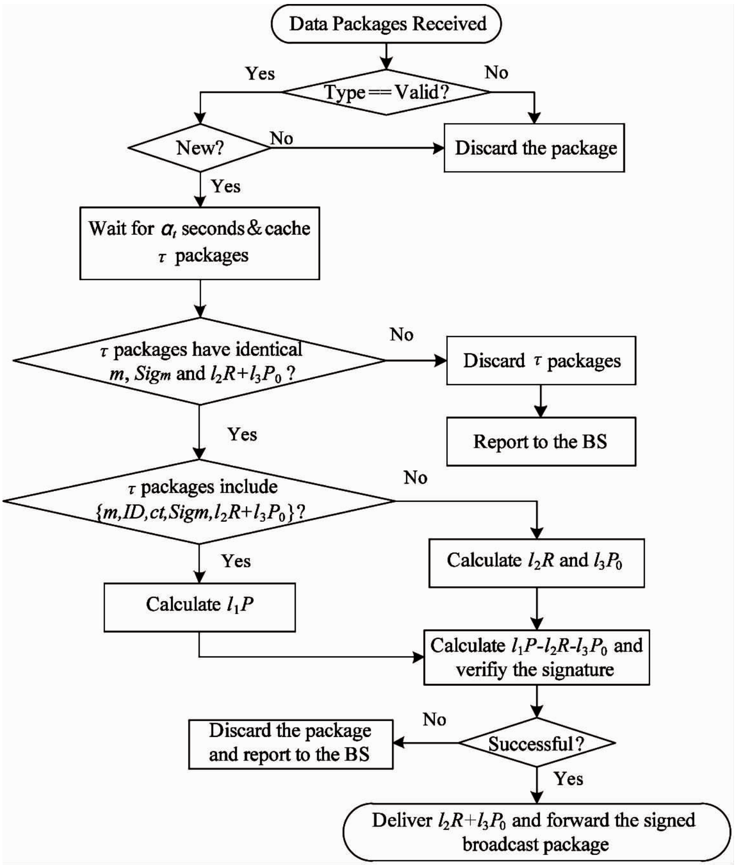
Data Packages Received
Yes
Type==Valid?
No
New?
No
Discard the package
Yes
Wait for α_t seconds&cache τ packages
τ packages have identical m, $Sigm$ and $l_2R+l_3P_0$?
No
Discard τ packages
Report to the BS
Yes
τ packages include $\{m,ID,ct,Sigm,l_2R+l_3P_0\}$?
No
Yes
Calculate l_2R and l_3P_0
Calculate l_1P
Calculate l_1P-l_2R-l_3P_0 and verifiy the signature
No
Discard the package and report to the BS
Successful?
Yes
Deliver l_2R+l_3P_0 and forward the signed broadcast package

Fig. 2 The process of OvBNN authentication mechanism

E_s, E_r and E_{mul} indicate the energy consumption by sending, receiving and calculating once multiplication respectively. Assuming that each node has η neighbors, the energy consumption of the optimized authentication mechanism OvBNN can be roughly estimated as

$$\overline{E} = \sum_{T=1}^{N} P_T(T \cdot E_S + \eta T/2 \cdot E_r - \eta T \cdot E_{mul}) \qquad (6)$$

In Eq. (6), $T \cdot E_S$ represents the energy consumed by T nodes transferring the intermediate calculation results, $\eta T/2 \cdot E_r$ is the energy consumed by $\eta T/2$ nodes receiving the intermediate calculation results, and $\eta T \cdot E_{mul}$ is the energy saved by $\eta T/2$ nodes performing the operation of multiplication twice. A suitable P_{rel} should be selected to minimize the energy consumption if the final value of $\overline{E}$ is positive.

4 Simulation results and performance analysis

The theoretical analysis is completed in the structure as shown in Fig. 3 with the assumption that there is no attack in this case. The node will send the intermediate results $hR + hcP_0$ to its neighbors. Simulating experiments are performed in a 4 ×4 grid network, under the premise of using MICAz node as the sensor node in the TinyOS system.

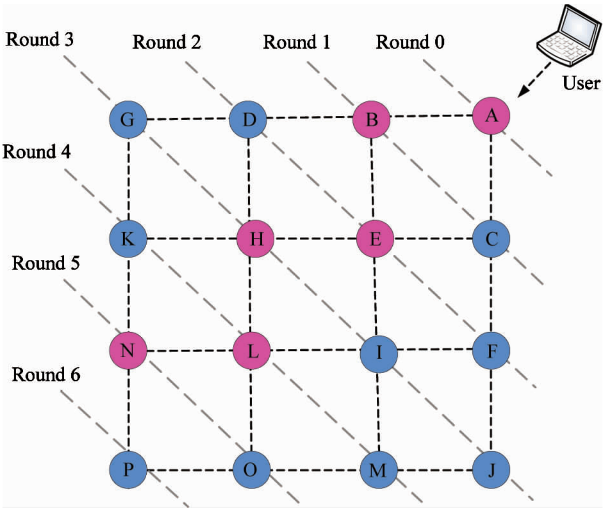

Fig. 3 4 ×4 grid structure in OvBNN

4.1 Theoretical analysis

The validity of the OvBNN mechanism will be analyzed in energy cost as well as the time cost in this section. In network deployment, MICAz nodes are adopted with 8-bit processors and ATmega128L microcontrollers working in 8MHz. According to Ref. [10], the time required of one multiplication will be about 0.81s. The working voltage of MICAz nodes is 3V, the current loss for transmitting data is 17.4mA and receiving data is 19.7mA, and the data transmission rate is 250kbps. IEEE802.15.4 is used as the MAC protocol for each node. The topology of the sensor node is shown as in Fig. 3. In order to make the safety strength of OvBNN equal to that of RSA with 1024bit, the size of packets settings are shown in Table 4.

Table 4 Size of packets settings

Parameter	Size	Parameter	Size
pt	2B	$hR + hcP_0$	42B
m	10B	Signature	83B
ID	2B	$\{m, ID_u, pt, Sig_m, hR + hcP\}$	139B

In Table 4, since the size of the data packet $\{m, ID_u, pt, Sig_m, hR + hcP_0\}$ has exceeded the transmission range, data packet will be divided into two parts to deliver.

It will cost each MICAz node E_{s1} and E_{r1} to send and receive 1B data respectively. From above, there will be

$$E_{s1} = 3.0 \times 17.4 \times 8/250 = 1.67\mu J \quad (7)$$

$$E_{r1} = 3.0 \times 19.7 \times 8/250 = 1.89\mu J \quad (8)$$

The energy consumption for authentication will be E_{ver} =58.32mJ, and once multiplication will cost E_{mul} =3.0 ×8.0 ×0.81 =19.44mJ. According to this, it will cost E_s = 3.0 × 17.4 × 128 × 8/250 =0.214mJ and E_r = 3.0 × 19.7 × 128 × 8/250 = 0.466mJ to transmit and receive the intermediate calculation results $hR + hcP_0$ respectively.

In the 4 ×4 grid structure deployed as shown in Fig. 3, it is not necessary for all nodes to transmit their intermediate calculation results to the neighbors. When being requested, node A will send the intermediate result to node B and node C. While B will transmit the intermediate results to D and E for fast authentication, node B and C will complete the authentication in the first round and turn in to the sleep mode to save energy. Nodes D, E, F will complete their certifications in the second round. Due to the deployed location of node E, it will send the intermediate result to nodes H and I. Node H then send its intermediate result to nodes K and L. In this way, 16 nodes will complete the authentication in 6 rounds, during which there will be 6 nodes consuming their own energy to speed up the authentication. Moreover, it will cost the energy of 11 nodes to receive the intermediate results. Therefore, the sending energy consumption is $E_{cost(s)}$ =6 ×0.124 =1.284mJ and the receiving will be $E_{cost(r)}$ = 11 × 0.466 =5.126mJ. The energy saving by the 11 nodes receiving $hR + hcP_0$ will be E_{sav} = 11 × 2 × 19.44 = 427.68mJ. Thus, in such 4 ×4 grid topology with 16 nodes, OvBNN can save the energy by E_{theo} =427.68 −1.284 −5.126 =421.27mJ, while the traditional vBNN will consume 16 ×58.32 =933.12mJ theoretically, which suggests that energy consumption by the proposed mechanism OvBNN will be 45.15% lower than that of vBNN.

4.2 Simulation results analysis

The proposed OvBNN signature authentication mechanism is analyzed in this part. NesC language-based applications in the TinyOS system are adopted to send and receive data packets[11]. The working state of sensors will change during the operation so as to save the limited energy. The transmission and reception of packets will also consume energy. Therefore, the simulation will compare the energy consumption from state changes as well as the energy consumption from packets transmission and reception between the proposed mechanism OvBNN and the traditional mechanisms including vBNN, ECDSA and FECDSA (Fast ECDSA).

4.2.1 Simulation analysis on different working states

Considering the small size of sensors and limited battery power, the node has to work in active state and sleeping state periodically to save energy. Wireless communication module in the sensor node often has four states: sending, receiving, idle, and sleeping. Sending and receiving processes are referred to as the active state. Idle state refers to that the node has to keep listening to the wireless channels, so idle state will still cost a lot energy[12]. In sleeping state, the node will turn off its communication module to minimize energy loss. The energy consumed by nodes in different states is different and Fig. 4 shows the proportion of energy consumption of nodes in different states.

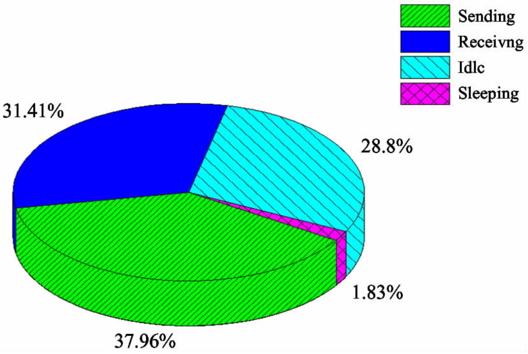

Fig. 4 Energy consuming ratio in different states

Fig. 5 depicts the states changing of a node. The initial state of the node is set to be idle, then the node turns into active state if it determines to receive data packets by monitoring, and enters the sleeping state after the completion of the authentication or task to save energy[13].

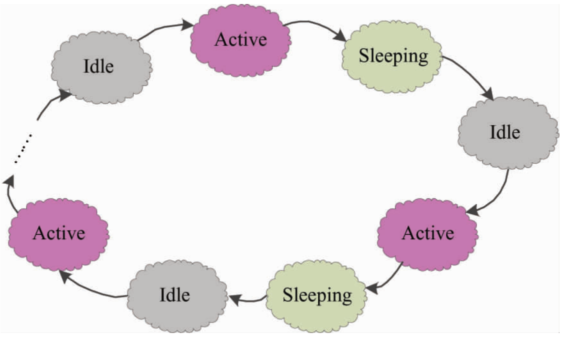

Fig. 5 Different states of the node

The simulation result from the perspective of node's states is shown in Fig. 6. It will cost the traditional vBNN about 42.79J to complete the certification process. The same process will cost ECDSA, FECDSA about 43.46J and 36.49J respectively. In contrast, the total energy cost by OvBNN is only 27.26J. On the other hand, it will take 25.17s for OvBNN to finish the authentication, while the time consuming is 50.30s, 53.87s, 39.60s for vBNN, ECDSA and FECDSA respectively.

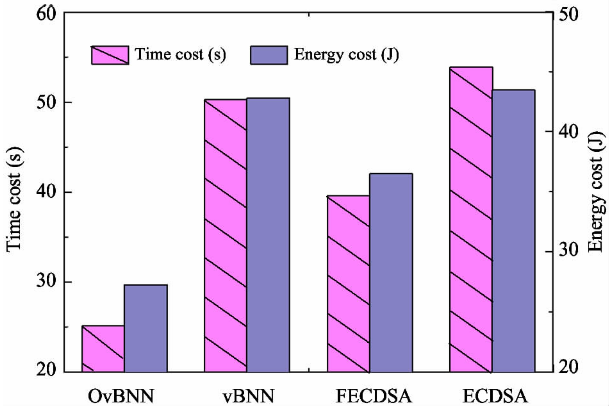

Fig. 6 Time and energy cost comparison for a whole work period

Obviously, Fig. 6 shows that OvBNN has distinct advantages compared with the other three mechanisms. The energy consumption by OvBNN is about 36.29% and 25.29% lower than that by vBNN and FECDSA. In the term of authentication efficiency, OvBNN will save 49.96% and 36.44% performing time in contrast with vBNN and FECDSA, respectively. Experiments show that the proposed mechanism OvBNN can shorten the required authentication time and save the energy effectively, thus extending the network life.

4.2.2 Simulation analysis on data delivering

The simulation uses MICAz as the sensor node in the verification. Since the node can transmit up to 128B of data packets in physical layer and the data packets with intermediate results $\{m, ID_u, pt, Sig_m, hR + hcP_0\}$ are 139B, the data packet is divided into two subpackets PAC_1 and PAC_2 as $PAC_1 = \{m, ID_u, pt, Sig_m\}$ and $PAC_2 = \{hR + hcP_0\}$. Projective Coordinate System (PCS) is applied, and the energy consumed by once multiplication is 51.795mJ and the time consumption is 1958ms with $SW = 3$ (The size of sliding window is 3). When the node sends the first packet, it will cost the energy by $E_{(s)PAC_1} = 491.4\mu J$, and $E_{(s)PAC_2} = 387.1\mu J$ for the second packet. When PAC_1 and PAC_2 are received, the energy consumed will be $E_{(r)PAC_1} = 598\mu J$ and $E_{(r)PAC_2} = 467\mu J$, respectively.

As shown in Fig. 7, vBNN, ECDSA and FECDSA consume 2503mJ, 3343.52mJ and 2783.3mJ, respectively, while the OvBNN mechanism only consumes 1371mJ. In terms of time consumption, it only takes OvBNN 2228s to complete the whole authentication. In contrast, it takes the other three mechanisms 6699ms, 6863ms and 4797ms, respectively. The comparison shows that OvBNN saves 45.22% energy and 66.74% time cost compared with the traditional vBNN, 50.47% and 53.55% respectively compared with FECDSA.

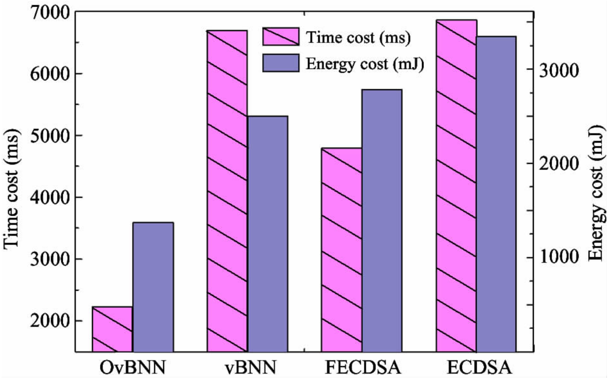

Fig. 7 Time and energy cost comparison for data delivering

From the simulation results above, it shows obviously that the proposed OvBNN signature mechanism is superior to the other three mechanisms in both energy cost and time delay. The saved energy and time delay will extend the whole network life effectively.

4.3 Performance analysis under classical attacks

4.3.1 Performance analysis under independent attacks

Suppose that there are independent attackers presented in WSN with a 4 × 4 grid. Then, each false packet will be received by two nodes during the next round of communication. Node D and node F are designated as the malicious nodes with being independent of each other so as to maximize the attack. In this case, nodes B, C, D, F and G shown in Fig. 3 will only receive one packet from their neighbors and perform signature authentication. Nodes E, H, I, K, L, N, O and P will keep the two packets from their neighbors and determine whether the security certification should be performed. In such condition, nodes A, B, E, H, L and N are still expected to send the intermediate calculation results to their neighbors as in subsection 4.1.

In this case, it will take $1.284 + 5.126 = 6.410$mJ to send and receive the intermediate result $hR + hcP_0$. Node H and node I will receive two different packets for node D and node F are malicious nodes. These two nodes (H and I) will complete the signature authentication themselves rather than using the intermediate results of node E. In this way, there will be six nodes using the intermediate calculation results to speed up the certification, which will save energy by about $6 \times 2 \times 19.44 = 233.28$mJ. Compared with the traditional vBNN, OvBNN will save the energy by at least $(233.28 - 6.410)/(14 \times 58.32) = 27.79\%$ when there are two mutually independent attackers in network. Meanwhile, the false packets sent by the malicious nodes will be discarded in the subsequent communication round and will not affect the network security.

4.3.2 Performance analysis under collusive attack

Suppose there are interdependent malicious nodes existing in WNS with a 4 × 4 grid as shown in Fig. 3. Node H and node I are set to be the collusive attackers and the false packets they sent are the same. Despite node L will receive the same packet from two malicious nodes and send it to node I and O, node N and O will perform signature verification themselves and will discard the false packet from node L due to the reception of two different packets.

In this condition, it will cost $1.284 + 5.126 = 6.410$mJ to send and receive $hR + hcP_0$. Since node H and node I are malicious nodes, node L will be captured to send false packets to node N and node O. Nodes N and O will perform signature verification by themselves instead of using the intermediate results to speed up the authentication. So there are 5 nodes using the intermediate calculation results to complete the certification in the whole process, which will save about $5 \times 2 \times 19.44 = 194.4$mJ. Compared to the traditional vBNN, OvBNN will save energy by $(194.4 - 6.410)/(14 \times 58.32) = 23.02\%$ when there are collusive attacks. OvBNN makes the security threat of malicious nodes be excluded from the subsequent authentication process effectively so as to avoid serious impact on the network.

5 Conclusion

The wide use of WSN makes the security problems be one of the most important issues in relative research area. Identity authentication is the basis of network security. The overhead and energy consumption caused by authentication cannot be ignored especially for WSN. An OvBNN is presented based on traditional vBNN by sending the intermediate calculation results to the neighbor nodes so as to speed up the authentication. The 4 × 4 grid structure is adopted to analyze the authentication process. To verify the effectiveness of the proposed OvBNN, the energy and time consumption for nodes in different states and for packets delivering are taken as the performance metrics. Compared with three other classical authentications, OvBNN will save more energy and time obviously in the condition with mutual independent attacks and collusive attacks.

References

[1] Muhammad A A, Peyman T, Nasser Y, et al. An efficient medium access control protocol for WSN-UAV[J]. *Ad Hoc Networks*, 2016, 52: 146-159

[2] Habib M, Antonio M, Valerio P. A sleep scheduling approach based on learning automata for WSN partial coverage[J]. *Journal of Network and Computer Applications*,

2017, 80(C): 67-78

[3] Ayaz H M, Ummer I, Mohiuddin B G. SPINS: mutual entity authentication protocol based on ECDSA for WSN [J]. *Procedia Computer Science*, 2016, 89: 187-192

[4] Conti M, Pietro R D, Spognardi A. Clone wars: Distributed detection of clone attacks in mobile WSNs[J]. *Journal of Computer and System Sciences*, 2014,80(3): 654-669

[5] Cristina A, Javier L, Rodrigo R, et al. Selecting key management schemes for WSN applications[J]. *Computers & Security*, 2012, 31(8): 956-966

[6] Fan X X, Gong G. Accelerating signature-based broadcast authentication for wireless sensor networks[J]. *Ad Hoc Networks*, 2012, 10(4): 723-736

[7] Elhoseny M, Eliminir H, Riad A, et al. A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption[J]. *Journal of King Saud University-Computer and Information Sciences*, 2016, 23 (3): 262-275

[8] Shankar S K, Tomar A S, Tak G K. Secure medical data transmission by using ECC with mutual authentication in WSNs[J]. *Procedia Computer Science*, 2015, 70: 455-461

[9] Cao X F, Kou W D, Dang L J, et al. IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks[J]. *Computer Communications*, 2008, 31 (4): 659-667

[10] Babamir F S. Implementation of aggregate signcryption in unattended medical WSNs using Micaz[J]. *International Journal of Electronics Mechanical and Mechatronics*, 2016, 6(2): 1123-1135

[11] Dalton A R, Hallstrom J O. nAIT: A source analysis and instrumentation framework for nesC[J]. *Journal of Systems and Software*, 2009, 82(7): 1057-1072

[12] Zhang S, Meng J E, Zhang B H, et al. A novel heuristic algorithm for node localization in anisotropic wireless sensor networks with holes[J]. *Signal Processing*, 2017, 138: 27-34

[13] Bruno M, Manuel R. Energy-efficient node selection in application-driven WSN[J]. *Wireless Networks*, 2017, 23 (3): 889-918

Qin Danyang, born in 1983. She received her B. Sc. degree in communication engineering from Harbin Institute of Technology in 2006, and both M. Sc and Ph. D. degrees in information and communication system from Harbin Institute of Technology in 2008 and 2011 respectively. Currently, she is an associated professor at the Department of Communication Engineering of Heilongjiang University, Harbin, P. R. China. Her researches include wireless sensor network, wireless multihop routing security and ubiquitous sensing.