International Journal of Computer Science and Business Informatics

IJCSBI.ORG

An Efficient Access Control Model for Wireless Sensor Network

Behzad Molavi
Department of Computer Engineering, University of imam raze, Mashhad, Iran
MSc. Student in Network Security

Hamed Bashirpour
Department of Computer Engineering, University of imam raze, Mashhad, Iran
MSc. Student in Network Security

Dr. Morteza Nikooghadam
Department of Computer Engineering, University of imam raze, Mashhad, Iran
Assistant Professor

ABSTRACT

The sensor nodes after a time lose their energy. In this case, to maintain network performance, new nodes can be added to the network. In the critical applications, the adversary can take advantage of this opportunity, and enter hostile node to the network. To prevent hostile node entry, an access control mechanism is needed. In this paper, a model for access control based on elliptic curve cryptography is proposed. The scheme makes sure the node authentication. Moreover, it has secure and fast method for key distribution. Evaluation shows that our efficient scheme compared to other models have less Computational overhead. Another feature of this model is robustness against denial of service attack.

Keywords: Sensor nodes, Adversary, Hostile node, Access control, Elliptic curve cryptography, key distribution, Denial of service, Node authentication.

1. INTRODUCTION

Wireless sensor networks are being developed. Due to the wireless nature of wireless sensor networks these networks used in many war zones and seismic monitoring environment. Sensor nodes usually have limited memory, small size and low processing power, and its energy are limited. Implement complex encryption algorithms in these networks is very hard. Sent and received on this network is broadcast to all. Thus one can easily receive packets from wireless channel. Access control is mechanism for the prevention of security attacks on wireless sensor networks. Secure access control caused by use of network resources is performed only by authorized nodes. Before sending, each node will receive their certificates from a unit trust. After receiving the certificate, new node can provide a secure connection with itself neighbors. This access control provide, both authentication and confidentiality requires. In addition to this scheme is robust against denial of service. In this paper we use ECDLP[1] algorithm for

[1] Elliptic Curve Discrete Logarithm problem

issuing and verifying certificates. Because the ECDLP faster than other methods such as the ECDSA[2].

2. RELATETED WORK

In 2002 SPINS protocol was introduced. The protocol is for data origin authentication [1]. The main drawback of this protocol is high additional overhead. Model for key distribution in the sensor networks provided in 2004. These models are only resistant to external attacks and in the internal attacks are very disabling [2]. In 2007, Yun Zhou et al.'s was introduced, an access control model in wireless sensor network [3]. Although Yun Zhou et al.'s model is perfect, but dos[3] attack can run it, In addition, the proposed model is faster in the generation and distribution of key. In 2009 Huang presented an access control model. Huang's method wasn't dynamic. Moreover, Huang's method is insecure [4].

3. REVIEW OF ATTACKS

Any enemy can be directly deployed malicious nodes in environment. In this case hostile node can hear messages from the other nodes, or inject false messages into the network. Note to figure 1. for further understanding.

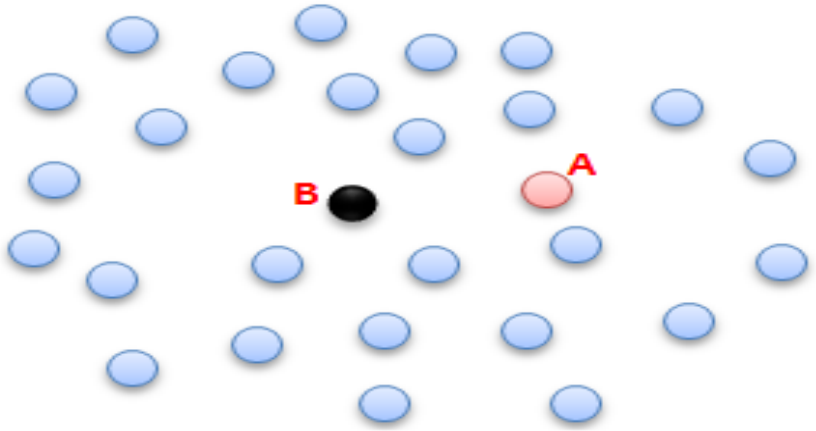

Figure 1. hostile node injection

In the figure 1, *B* is a hostile node. It can Fake data, or inject bogus data into the network.

In the sybil attack, an enemy node could fake the identity of an authorized node and introduces itself instead of another node. Figure 2. provides further understanding.

[2] Elliptic curve digital signature algorithm

[3] Denial of service

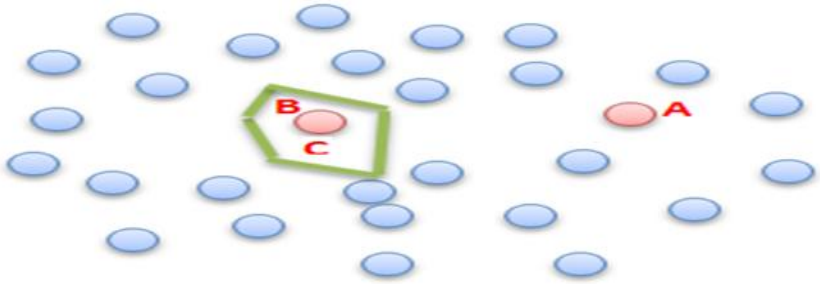

Figure 2. Sybil attack

In the figure 2, B node forge C node's Identity.

In this attack an enemy get confused routing algorithm. In the wormhole attack, hostile receive packets from the network then sends the packets to the other side in the network. This detour reduces performance. Figure 3. provides further understanding.

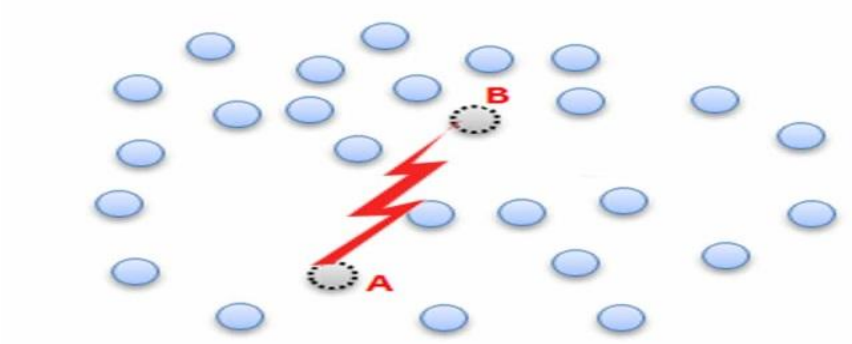

Figure 3. Wormhole attack

In the figure 3, A detour has been established between A and B.

Enemy sends waste packets to authorized nodes. In this case authorized nodes do not have ability to service. Note to figure 4. for further understanding.

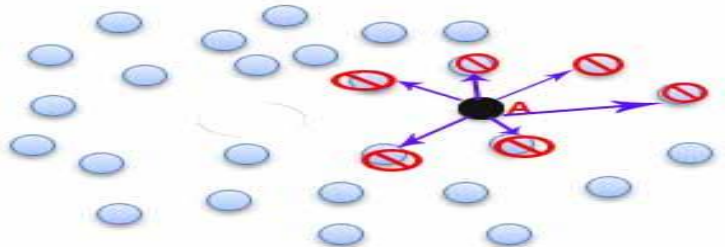

Figure 4. DOS attack

4. ASSUMPTIONS

In this scheme, all sensor nodes are same, the range sending all sensor nodes are similar. public and private keys generated for each sensor node is done by CA[4]. All the sensor nodes are programming by the CA before being placed on the network. After key generation phase for each new nodes, CA considers the current time as the timestamp. This timestamp is called T_i . Nodes were fixed in the network. This assumption makes sure that we have fixed neighbors. In this access control model for each neighbors node connection, we have key. For example if a node has 10 neighbors, then it should be has 10 keys. posts in wireless networks are many to one. In fact, all the sensor nodes will be sent the received data to the sink. To better understand the issue notice in figure 5.

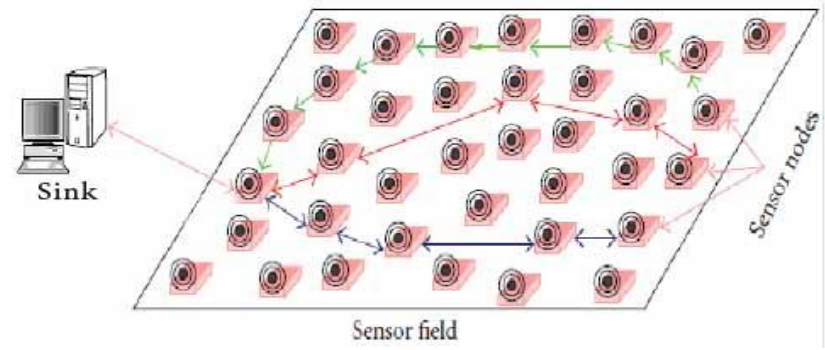

Figure 5. Sensor network [8]

5. PROPOSED SCHEME

The main scheme takes place in two phases. In this scheme we use elliptic curve cryptography tools. The first phase, pre deployment is called. In this phase elliptic curve parameters such as base point, and the elliptic curve equation coefficients are calculated. For better understanding, read mathematical preliminaries from the paper [6]. The second phase is related to the distribution of nodes in the network

5.1 PRE DEPLOYMENT PHASE

First coefficient elliptic curve and base point are determined. Here we use the notation G for the base point. We assume that the order of elliptic curve is n. then, CA select own private key from $[1, n-1]$. We show CA's private key with k notation. The public key of the CA denote by the symbol Q. CA's public key is obtained from equation 1.

$$Q = kG \qquad k \in [1, n-1] \qquad (1)$$

According to the elliptic curve problem, obtain k Based on Q and G is very difficult. Generate public and private keys of other nodes are similar to CA.

[4] Central authority

Here the node's private key denoted by the symbol d_i. Nodes are chosen own private key from the range $[1, n-1]$. Node's public key denoted by the symbol P_i. Node's public key is obtained from equation 2.

$$P_i = d_i G \qquad d_i \in [1, n-1] \qquad (2)$$

CA considers T_i as key generation time. For each node CA selects a random number that denote by symbol W_i. Then CA Takes F_i from equation 3.

$$F_i = W_i G \qquad F_i = (x_i, y_i) \qquad (3)$$

Each F is a point on the elliptic curves and it's has two-dimensional (x_i, y_i). For each new node, CA determines a time for concatenation new nodes to network that denote by symbol L_i. For each node the values $N_i + P_i + T_i + L_i$ append with together and then put it in a hash function. Note to equation 4 for further understanding.

$$e = H(N_i + P_i + T_i + L_i) \qquad (4)$$

According to equation 5, the certification of each node will be produce. In fact, the pair of $< S_i, F_i >$ is considering as certification.

$$S_i = (d_i x_i e + W) \qquad (5)$$

Finally CA defines feature behavior such as threshold for packets sending and operating frequency in the network for each node. These behavioral parameters denote by symbol B.

5.2 NODE DEPLOYMENT PHASE

When a new node enters to network, the new node broadcast ($N_i P_i T_i L_i < S_i, F_i >$). The Neighbors must be Check integrity of new node and develop a session key. Neighbors of the new node, follow these steps.

1. After receiving request from a new node, old node checks behavioral parameters B. If these parameters were unusual, then this request will reject.
2. Old node compare time stamp $|T_i - t|$ with L_i. That the t is current time. If the new code violated permitted range, then old node reject request of new node.
3. Old node checks certificate of the new node. If it's not valid, then old node reject request of new node.
4. Old node encrypt own certificate with a nonce by session key, and then sent cipher text to new node.
5. New node compute session key and then decrypt cipher text by session key.
6. New node verifier old node certificate.
7. New node encrypts a nonce by session key, and then sends this message to old node.

For better understand we show this hand shake between new node and old node in the figure 6.

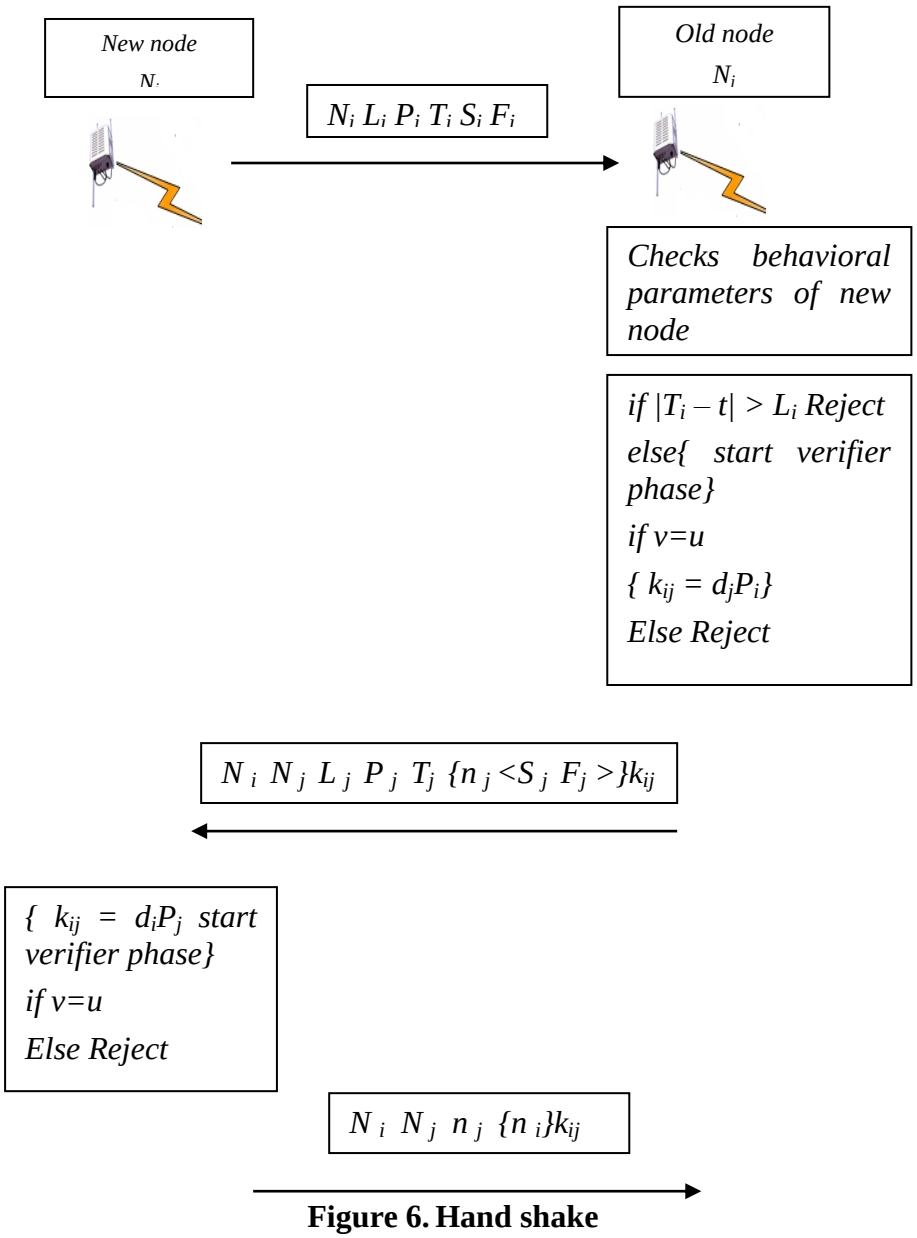

Figure 6. Hand shake

Each node can checks certificate by compute two variable in the equation 6 and 7. If $V = U$, then the certificate is valid. For more understanding, note to equation 6 and 7 and 8.

$$V = S_i G \quad (6)$$

$$U = e\, x_i P_i + F_i \quad (7)$$

$$V = SG = (d_i x_i e + K)G = e\, x_i P_i + F_i \quad (8)$$

Note that, each node can compute session key by own private key and others public Key. For more understanding, note to equation 9.

$$K_{ij} = d_i . P_j = k_{ji} = d_j . P_i \quad (9)$$

6. SECURITY ANALYSIS

6.1 HOSTILE NODE INJECTIONS AND SYBIL ATTACK

Each node need to certificate for accession to network. Produce certificate is done just by CA in the pre deployment phase. And forge a certificate is a hard problem, because it's based elliptic curve problem.

6.2 WORMHOLE ATTACK

In this method we define some behavior for each node. One of these behaviors is distance post. The distance post can Estimate by signal parameter such as power signal, frequency and so on. If each node do impinge at the radio basin then probability exist wormhole channel, so other nodes reject this node.

6.3 DOS ATTACK

Exchange information done by session key. In this model when a node sends data to neighbors, the neighbors can find out which node sends data and can compute the number request in each time scale. If the request number impinge of behavioral threshold then other node reject this node to avoid dos attack. For more understanding, note to table 1.

Table 1. Previous methods

Previous methods	Not forging probability	Resistant to DOS	Being dynamic	Tracing
Wu et.' al 2001	Yes	No	No	No
Jeng Wang 2006	Yes	No	No	No
Zhou fang et.' al 2007	Yes	No	Yes	Yes
Fan Wu et al.'s 2012	Yes	No	Yes	No
Our schema	Yes	Yes	Yes	Yes

7. EVALUATION

For evaluation, we convert all operation to multiplying. Then we proof that our scheme has low computational overhead against previous methods. For more understanding, note to table 2.

Table 2. Convert operation

Operation	***Base multiplying***
Exponential functions	*240 T_{MUL}*
Multiplication on Elliptic Curve	*29 T_{MUL}*
Add on Elliptic Curve	*0.12 T_{MUL}*
Add	*Negligible*
Hash	*Negligible*

In our proposed schema, we use ECDLP instead of ECDSA. In the Zhou fang's model, they use ECDSA for verifier [3]. In the table 3 we show that ECDSA has low less computational overhead.

Table 3. Evaluation

Method	***Mathematical expression***	***Time complexity based mul***
ECDSA	$2T_{MUL}+T_{INV}+T_{EC\text{-}MUL}+T_{HASH}$	$60.12\ T_{MUL}+ T_{INV.HASH}$
ECDLP	$2T_{MUL}+ T_{EC\text{-}MUL}+ T_{HASH}$	$59.12\ T_{MUL}+T_{HASH}$

8. CONCLUSIONS

In this paper we introduce an access control for wireless sensor network. We use ECDLP method for verifying certificate of nodes, because it's have low overhead computation. Moreover in this schema we define some behavior for each node, to avoid dos attack and worm hole attack. This method Compared with previous method is more efficient and robust against dos attack.

REFERENCES

[1] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, D.E. Culler, SPINS: Security protocols for sensor networks, Wireless. Networks 8 (September) (2002) 521–534.

[2] Y. Zhang, W. Liu, W. Lou, Y. Fang, Location-based compromise-tolerant security mechanisms for wireless sensor networks, IEEE JSAC, Special Issue on Security in Wireless Ad Hoc Networks 24 (2) (2006) 247–260.

[3] Y. Zhou, Y. Zhang, Y. Fang, 2007. Access control in wireless sensor networks. Ad Hoc Networks 5 (1), 3–13.

[4] H.F. Huang, 2009. A novel access control protocol for secure sensor networks. Computer Standards and Interfaces 31 (2), 272–276

[5] Wu. Fan, Pai. Hao-Ting, An adaptable and scalable group access control scheme, Telematics and Informatics 2012

[6] M. Nikooghadam, A. Zakerolhosseini, Efficient Utilization of Elliptic Curve Cryptosystem for Hierarchical Access Control, system and software jurnal 2010

[7] X. Zou, Y.S. Dai, E. Bertino, 2008. A practical and flexible key management mechanism for trusted collaborative computing. In: Proceedings of the IEEE Conference on Computer Communications (INFOCO, 2008), April, Phoenix)

[8] B. Antoine, B. Bagula, Modelling and Implementation of QoS inWireless Sensor Networks, *Intelligent Systems and Advanced Telecommunication*, 12 June 2010

[9] M. Nikooghadam, A. Zakerolhosseini, a protocol for digital sinnature based ECDLP, 2008 asian network jurnal

[10] M. Nikooghadam, F. Safaei & A. Zakerolhosseini. (2010). An efficient key management scheme for mobile agents in distributed networks, In *IEEE, 1st international conference on parallel, distributed and grid computing*.

[11] M. Nikooghadam, & A. Zakerolhosseini. (2009). An efficient blind signature scheme based on the elliptic curve discrete logarithm problem. *The ISC International Journal of Information Security, 1*(2), 125–131.

[12] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, 2002. Wireless sensor networks: a survey. Computer Networks 38 (4), 393–422.

[13] Abbasi, A.A., Younis, M., 2007. A survey on clustering algorithms for wireless sensor networks. Computer Communications 30 (14–15), 2826–2841.

[14] Y. Kim, A. Perrig, G. Tsudik, 2004. Group key agreement efficient in communication. IEEE Transactions on Computers 53 (7), 905–921.