Simple Hash Based Message Authentication Scheme for Wireless Sensor Networks

Abror Abduvaliev
Dept. of Comp. Eng,
KyungHee University,
Suwon, Korea.
abror@oslab.khu.ac.kr

Sungyoung Lee
Dept. of Comp. Eng,
KyungHee University,
Suwon, Korea.
sylee@oslab.khu.ac.kr

Young-Koo Lee
Dept. of Comp. Eng,
KyungHee University,
Suwon, Korea.
yklee@khu.ac.kr

Abstract – **In this work, we propose simple hash based message authentication and integrity code algorithm for wireless sensor networks. The proposed scheme uses pre-shared secret key which is obtained from Elliptic Curve Diffie Hellmann (ECDH) key exchange algorithm, and is based on modified SHA-1 (mSHA-1) hash function which helps to compute message authentication code for given messages. We suggest two scenarios depending on scale of the network, and also analyze security of the proposed algorithm. This algorithm provides both integrity and authenticity of a message with only one hash value.**

Keywords – authentication, keyed hash function, wireless sensor networks

I. INTRODUCTION

Wireless sensor network (WSN) applications are the fast growing technology trend but security and privacy is still largely ignored, since they are hard to achieve given the limited computation and energy resources available at sensor node level. However, secure communication is a requirement for many WSN applications to ensure integrity and authenticity of transmitting data. In many cases it is sufficient to secure data transfer between the sensor nodes and the base station. In particular, the base station must be able to ensure that the received message was sent by specific sensor node and not modified while transferring. Many WSN applications such as health-care monitoring systems or military domains needs strong and lightweight authentication schemes to secure data from unprivileged users. The authenticity and integrity of messages received by base station greatly influence final tracking results [1, 2].

In this paper, we propose a new hash based authentication scheme for wireless sensor networks which reduces the computational overhead of sensor nodes and produces strong unique message authentication code (MAC) for a particular message. SHA-1 hash function modified with the help of regularly distributed pseudo random function [10] which provides collision resistant requirement for hash functions and the pre-shared secret key obtained from ECDH secret key exchange algorithm. The main goal of this work is to reduce communication and computation overheads while achieving strong and secure authentication scheme for wireless sensor networks. Also, the scheme can be designed as an extendable algorithm to prevent flooding and forgery attacks from malicious and unauthorized sensor nodes.

The rest of this paper is as follows. In section 2, we discuss about previous works on MAC based authentication schemes for WSN. The description of proposed scheme is given in section 3. The results with real examples and security of this scheme are shown in section 4. Finally, section 5 concludes the paper with discussing the future work as well.

II. RELATED WORKS

Message authenticity and integrity is a critical issue for network security, as network must guarantee the delivery of message without any modification or alteration. This consideration tends to be also one of the main issues of WSNs. There are some related works in MAC based authentication protocols for wireless sensor networks.

T. H. Lee [3] and Wong et al. [4] proposed strong password based authentication protocols which are almost similar to each other. These algorithms can reduce computational load and have reliable time synchronization but they are weak against user-password security attacks and not mentioned about which MAC algorithm to use.

T. Yao et al. [5] described authentication protocol for broadcasting messages using one-way key chain and secure acknowledgements, but there is no time synchronization and even one malicious node can disrupt the whole broadcasting process because of unknowing key-chain.

Kim et al. [6] proposed the algorithm for detecting and dropping fabricated reports from representative nodes using message authentication codes. However, according to our knowledge, this scheme brings to communication overload due to number of MACs which are computed by representative nodes.

According to previous works and problems, our main target is decreasing computing power for authentication process with the help of message authentication code (MAC) algorithm which provides strong, unique and secure MACs.

III. THE PROPOSED SCHEME

In this section, we describe in detail simple hash based authentication scheme for wireless sensor networks.

A. ECDH

To implement MAC algorithm, we use pre-shared secret keys between sensor nodes and base station, which are obtained with the help of Elliptic Curve Diffie-Hellmann (ECDH) key exchange algorithm. ECDH is reliable algorithm in terms of energy consumption and communication overhead constraints of WSN. ECDH provides the same security level as normal Diffie-Hellmann with smaller key sizes. Security of this algorithm is based on Elliptic Curve Discrete Logarithm Problem. Within ECDH, a secret key K_s between sensor node and base station is established. The detailed description of this key exchange algorithm is given in [7].

B. Pseudo random function and using modified SHA-1 as a MAC

As we mentioned above, the authenticity and integrity of transmitting messages must be secure and easy to compute. The procedures below are the detailed explanation of our proposed scheme.

First, we list the notations and their corresponding definitions on Table 1.

TABLE 1. NOTATIONS

Symbol	Definition
K_s	The common key shared between sensor node and base station
K_S^X	The key stored on base station's database which is shared between sensor node X and base station
$F(w_i)$	Pseudo-random function in modified SHA-1 hash function
H	Modified SHA-1 hash function
$MAC_X(M)$	Message authentication code of sensor node X over message M
destAdr	Address of destination
||	Concatenation

We use modified SHA-1 hash function to compute message authentication code of a given message M. We made modification to SHA-1(mSHA-1) hash function using regularly distributed pseudo-random function. The detailed description of this algorithm is given in [10]. As we know, original SHA-1 uses logical functions on its main loop:

$$f_i(B,C,D) = (B \wedge C) \vee ((\neg B) \wedge D)$$

$$f_i(B,C,D) = B \oplus C \oplus D$$

$$f_i(B,C,D) = (B \wedge C) \vee (B \wedge C) \vee (C \wedge D)$$

$$f_i(B,C,D) = B \oplus C \oplus D$$

We changed these logical functions with pseudo-random function which gives unique hash values for a particular message due to its randomness and no repeating period. According to that algorithm, the pseudo-random function is: $F(w_i) = w_i * \sqrt{2}$ which is input value for the main loop in mSHA-1. We add secret key K_s to the function and it becomes as follows:

$$F(w_i) = w_i * \sqrt{2} * K_S \qquad (1)$$

Adding the secret key gives us the keyed hash function which can be used as a message authenticity and integrity code (MAC). The output value of hash function depends only on secret key and the input message. It means that only the holders of secret key can compute appropriate hash value for the message.

MAC of the message is computed as follows:

$$MAC_K(M) = H_k(M) \qquad (2)$$

In this paper, we suggest two scenarios according to network size of the application. We concatenate address of destination to the message in case of clustered WSNs and the formula becomes as follows:

$$MAC_K(M) = H_k(M \,\|\, destAdr) \qquad (3)$$

The length of hash value is 160-bit the same as SHA-1.

The Figure 1 is the pseudo code of the proposed algorithm.

```
START
s : compute $MAC_K(M) = H_K(M)$
s : transmit M and $MAC_K(M)$ to basestation
b : get M and $MAC_K(M)$
b : compute $MAC'_K(M) = H'_K(M)$
b : compare $MAC'_K$ and $MAC_k$
    IF $MAC'_K = MAC_k$ THEN
        m : Authenticated
    ELSE
        m : Unauthenticated
    ENDIF
END
```

Figure 1. The pseudo code of the algorithm

C. Scenarios:

For this algorithm we can propose two different scenarios according to the network size. Scenario 1 is for static or small-sized WSNs where numbers of sensor nodes are not huge. We suggest using clustered WSNs in case of a large number of sensor nodes in WSN. Scenario 2 can be used for big-scale applications where transmitted data goes to base station through cluster-head.

Scenario 1:

We assume that we have static WSN where sensor nodes can directly connect to the base station. Suppose, sensor node A has message M and pre-shared K_s secret key with base station.

1. Sensor node A computes MAC_A with the help of secret key over message M, and then sends it to a base station.
2. The base station computes $MAC_A^{'}$ of received message using the secret key K_S^A which is shared with sensor node A.
3. Then compares $MAC_A^{'}$ with received MAC_A; if result is appropriate, then the received message counts as an authenticated.

The overall handshake of this scenario is given in Figure 2. This scenario is suggested to small-scale applications where point to point communication is possible.

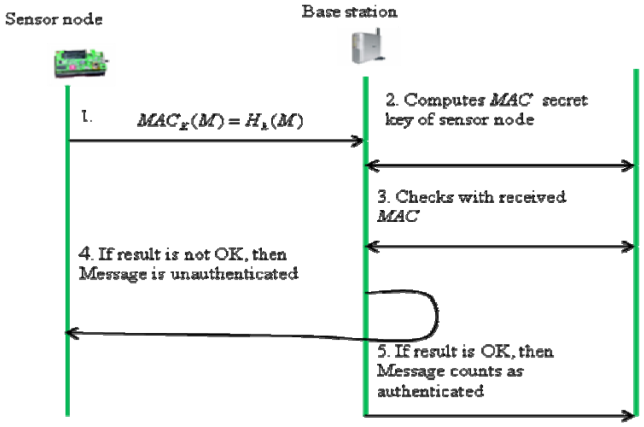
Sensor node
Base station
1. $MAC_K(M) = H_k(M)$
2. Computes MAC' secret key of sensor node
3. Checks with received MAC
4. If result is not OK, then Message is unauthenticated
5. If result is OK, then Message counts as authenticated

Figure 2. The overall handshake of this scenario 1.

Scenario 2:

We assume that we have a clustered WSN that is composed of a large number of sensor nodes, and the sensor nodes are able to organize a cluster automatically after deployment in a field of interest. Suppose, sensor node A has message M and pre-shared K_s secret key with base station.

1. Sensor node A computes MAC_A with the help of secret key over message M and destination address, and then sends it to a cluster-head.
2. Cluster-head has its own database of keys which are pre-shared between its cluster-nodes and base station. Cluster-head computes $MAC_A^{'}$ of received message using the common key K_s with sensor node A.
3. Then compares two MAC values; if result is appropriate, then forwards it to base station, otherwise the message counts as an unauthenticated and returns it to sensor node A.

The overall handshake of this scenario is illustrated in Figure 3. The advantage of using clustered WSNs is reducing communication overhead.

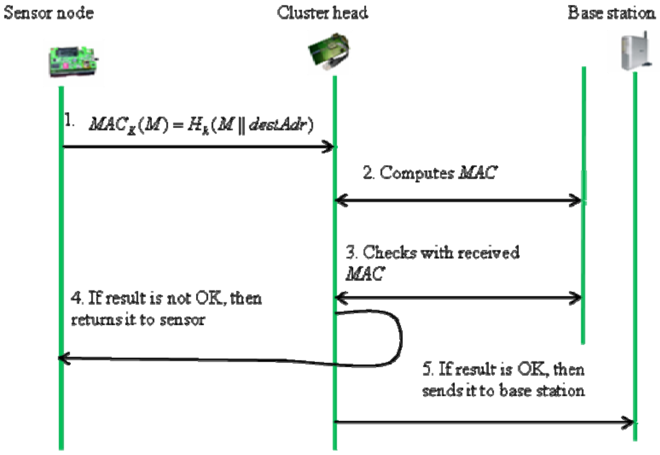
Sensor node
Cluster head
Base station
1. $MAC_K(M) = H_k(M \| destAdr)$
2. Computes MAC
3. Checks with received MAC
4. If result is not OK, then returns it to sensor
5. If result is OK, then sends it to base station

Figure 3. The overall handshake of Scenario 2

In this case, cluster–head stores only the pre-shared secret keys of its own clusters and base station. Sending message through cluster-head reduces number of communications and prevents flooding attack from malicious nodes.

IV. Analysis of Proposed Scheme

We analysis security of the proposed scheme in terms of uniqueness of the MAC value and a quantitative performance analysis with respect to communication and computation overheads in terms of energy consumption.

A. Security analysis

The proposed scheme is based on modified SHA-1 hash function which uses regularly distributed pseudo-random function. The randomness and no repeating period of this function give us unique hash values. By adding secret key we achieved the keyed hash function which can be used as a

MAC of message. Unauthorized users or attackers cannot calculate hash value of the message without knowing pre-shared secret key. Clustered WSNs helps to achieve one of our main goals which is to reduce the number of communications and prevent network flooding attack. Additionally, mSHA-1 fulfills the computational constraints of the sensor nodes. Cluster-head compares the received MAC with its own computed MAC for a received message, and reacts depending on result of comparison.

B. Efficiency Analysis

We will now shortly analyze the proposed algorithm with respect to energy consumption. As reported in [12], a Chipcon CC1000 radio device used in Crossbow MICA2DOT motes consumes 28.6 and 59.2 μJ to receive and transmit one byte, respectively, at an effective data rate of 12.4 kb/s. In TinyOS by default each message consists of 10 bytes header and a 29 bytes payload. In our case, the length of message authentication code is 20 bytes which includes address of destination. ZigBee specifies a maximum packet length of 128 bytes. Therefore the maximum payload is theoretically 100. We assume a packet of 128 bytes, 100 for the payload and 20 bytes for the header ensuing a 8-byte preamble, consists of source, destination, length, packet ID, CRC, and a control byte [12]. We also assume that the length of message M is 20 bytes. We can calculate the energy consumption E_S for sending and E_R receiving message M:

$$E_S = (20+20+8)*59.2 = 2.84\text{mJ};$$

$$E_R = (20+20+8)*28.6 = 1.37\text{mJ};$$

If more than 100 bytes have to be transmitted the message has to be split and sent in chunks. The overhead for sending a payload of x total bytes can be estimates as follows:

$$p(x) = 28*[\frac{x}{100}] \tag{4}$$

The total energy consumption $E_T(x)$ for transmitting (i.e., receiving and sending) a message M of x bytes can be estimated as follows:

$$E_T(x) = (E_S + E_R)*(p(x)+x)*8\frac{b}{B} \tag{5}$$

Let's assume the length of message as 200 bytes and compute the total energy consumption:

1. $p(x) = 28*[\frac{200}{100}] = 28*2 = 56 \textit{ bytes}$
2. $E_S = (20*2+8*2+200)*59.2 = 15.15\text{mJ}$
3. $E_R = (20*2+8*2+200)*28.6 = 7.32\text{mJ}$
4. $E_T(x) = (15.15+7.32)*(56+200)*8/200 = 230.1\text{mJ}$

We have estimated energy consumptions for sending data from sensor node and receiving it by base station, and also calculated the total energy consumption in terms of overall communication for the message of 200 bytes. Some conclusions can be drawn from these analyses. First, the communication overhead is low compared to other related authentication schemes in section II. Second, MAC algorithm is based on strong and reliable keyed hash function which is impossible to compute appropriate hash values without knowing secret key.

V. CONCLUSIONS AND FUTURE WORKS

We have proposed a new approach for message authentication in wireless sensor networks. The proposed scheme is based on modified SHA-1 hash function by using regularly distributed pseudo random function. The reliable MAC algorithm provides both message authenticity and integrity for unique messages. We analyzed security and efficiency of the proposed scheme. Additionally, we suggested two scenarios according to the number of sensor nodes. In future, this scheme can be extended to as an intrusion detection system to detect and reject malicious nodes in wireless sensor networks by using MACs.

ACKNOWLEDGMENTS

This research was supported by the MKE (Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Advancement) (IITA-2009-(C1090-0902-0002)). This work also, was supported by the Korea Science & Engineering Foundation (KOSEF) grant funded by the Korea government (MEST) (No. 2008-1342), and was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2009-0076798). This work is supported by the IT R&D program of MKE/KEIT, [10032105, Development of Realistic Multiverse Game Engine Technology].

REFERENCES

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks, IEEE Communications Magazine," Vol. 40, No. 8, pages 102-116, August 2002.

[2] I. Akyildiz and I. Kasimoglu, "Wireless sensor and actor networks: research challenges," Ad Hoc Networks 2(4), pages 351- 367, 2004

[3] Tsern-Huei Lee, "Simple Dynamic User Authentication Protocols for Wireless Sensor Networks", Second International Conference on

Sensor Technologies and Applications (SENSORCOMM’08), pages 657-660, France, 2008

[4] K. H. M. Wong, Y. Zheng, J. Cao, and S. Wang, “A dynamic user authentication scheme for wireless sensor networks,” Proceedings of IEEE International Conference on sensor networks, ubiquitous, and trustworthy computing, pages 244-251, 2006

[5] Taketsugu Yao, Shigeru Fukunaga and Toshihisa Nakai, “Reliable Broadcast Authentication in Wireless Sensor networks”, LNCS, vol.4097, pages 271-280, 2006

[6] Byung Hee Kim and Tae Ho Cho, “Efficient selection method of message authentication codes for filtering scheme in sensor networks”, In the Proceedings of the 2nd international conference on Ubiquitous information management and communication, pages 511-514, 2008

[7] D. Malan, M. Welsh and M. Smith. “A Public Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography”, Proceedings of IEEE Sensor and Ad Hoc Communications and Networks (SECON04), Santa Clara, California, 2004

[8] H. Song, S. Zhu, W. Zhang and G. Cao, “Least privilege and privilege deprivation: Toward tolerating mobile sink compromises in wireless sensor networks”, ACM Transactions on Sensor Networks, Vol. 4, No. 4, 2008

[9] Huei-Ru Tseng, Rong-Hong Jan and Wuu Yang, "An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks", IEEE Global Communications Conference (GLOBECOM 2007, Washington, DC, USA), pages 986-990, Nov. 2007

[10] Abror Abduvaliyev, Sungyoung Lee and Yong-Koo Lee, “Modified SHA-1 hash function (mSHA-1)”, Proceeedings of ITC-CSCC2009, pages 1320-1324, Jeju, Korea, July, 2009

[11] B. Schneier, “Applied Cryptography”, John Wiley & Sons Inc., New York, 2nd edition, 1996

[12] Y. Zhang, W. Liu, W. Lou, and Y. Fang, “Location based security mechanisms in wireless sensor networks,” IEEE JSAC, Special Issue on Security in Wireless Ad Hoc Networks, vol. 24, no. 2, pp. 247-260, Feb. 2006

[13] Crossbow Technology Inc, http://xbow.com/, 2004