

An Efficient Identity Authentication Scheme for Wireless Sensor Networks

Joon Heo

School of Electronics and Information
Kyung Hee University
Seocheon, Giheung, Yongin, Gyeonggi, KOREA
heojoon@khu.ac.kr

Choong Seon Hong

School of Electronics and Information
Kyung Hee University
Seocheon, Giheung, Yongin, Gyeonggi, KOREA
cshong@khu.ac.kr

Abstract— Security and privacy protection are of extreme importance for many of the proposed applications of wireless sensor networks (WSNs). However, security in sensor networks is complicated by the lack of tamper-resistant hardware (to keep per-node costs low). In addition, sensor nodes have limited storage and computational resource. This paper proposes a lightweight identity authentication scheme at the link layer for data frame in WSNs. With the proposed scheme there are only n -bits for authentication, which can greatly reduce overhead and thus preserves the scarce wireless bandwidth resource. Statistical method proves that our scheme is successful in handling MAC layer attack.

Keywords-component; WSNs, lightweight authentication, synchronization algorithm, statistical attack detection

I. INTRODUCTION

Sensor networking has become an exciting and important technology in recent years. It provides an economical solution to many challenging problems such as traffic monitoring and building safety monitoring. Security and privacy protection are of extreme importance for many of the proposed applications of WSNs. The major challenges in tackling wireless sensor networks security include: power conservation for mobile sensors, cooperation among heterogeneous sensors, flexibility in the security level to match the application needs, scalability, self organizing and self learning capabilities of sensor, trust and security decisions for the application, keeping the mobility and volatility transparent, and yet protecting the network from external and internal intrusions. In a nutshell there are three factors that we have to consider energy, computation and communication [9]. Due to resource scarcity (battery power, memory, and processing power) of sensor, securing sensor networks is quite different from traditional schemes that generally involve management and safe keeping of a small number of private management and safe keeping of a small number of private and public key [10]. WSNs share several important properties with traditional wireless networks, most notably with mobile ad hoc networks. Both types of networks rely on wireless communication, ad hoc network deployment and setup, and constant changes in the network topology. Many security solutions proposed for wireless networks can be applied in WSNs; however, several unique characteristics of WSNs require new security scheme [7].

· **Limited resources.** Sensor network nodes are designed to be compact and therefore are limited by size, energy, computational power, and storage. The limited resources limit the types of security algorithms and protocols that can be implemented. Security solutions for WSNs operate in a solution space defined by the trade-off between resource spent on security and the achieved protection.

· **In-network processing.** Communication between the nodes in a WSN consumes most of the available energy, much less than sensing and computation do. For that reason, WSNs perform localized processing and data aggregation. An optimal security architecture for this type of communication is one in which a group key is shared among the nodes in an immediate neighborhood. However, in an environment in which the nodes can be captured, the confidentiality offered by the shared symmetric keys is easily compromised.

In this paper, we propose a lightweight identity authentication at the link layer for data frame in WSNs. Unlike traditional authentication scheme, the proposed scheme determines the legitimacy of a sender by continuously checking a series of data frames transmitted by the sender. The major purpose of the proposed scheme is to detect an attack in an error-prone wireless environment. When the base station detects an attack, some protection or anti-attack approaches for each type attack can be triggered. The proposed scheme identifies the attack by using a statistical way and provides access control. This paper is organized as follows. Section 2 includes related works. Section 3 describes the proposed scheme for identity authentication. Section 4 provides the statistical method. Finally, we give some concluding remarks.

II. RELATED WORKS

A. Authentication in Wireless Sensor Networks

At UC Berkeley, prototype networks of small sensor devices are developed under the SmartDust program. In this program a set of Security Protocols for Sensor Networks (SPINS) [11] are presented as μ TESLA and Secure Network Encryption Protocol (SNEP). The protocols will run under a special operating system, named TinyOS [12]. μ TESLA is designed to handle authentication between two devices and

authenticated broadcast. This is done with delayed key disclosure and one-way function key chains. These results show that adding security to a highly resource constrained sensor network is feasible and that security systems can be an integral part of practical sensor network.

B. Random-Bit Window-based Authentication Protocol

Lightweight per-packet authentication using only one bit was first presented in [3]. The idea of attaching random bits to each packet was borrowed to develop the RBWA protocol [5]. Since the RBWA protocol is in the IP layer it can work with various link layers and network topologies. The design of the RBWA is based on an identical random-bit stream generated with a shared session key and separated into blocks. Hereafter, each packet is associated with a random-bit block in order to gain the network access illegally. However, without knowledge of pre-shared session key the probability to guess the random-bit block correctly is dependent on the number of bits used for each block. The receiver then has to know which random-bit block that is associated with which packet. In order to achieve synchronization between the sender's and receiver's random-bit blocks, a unique sequence number generated by a counter is attached to each packet. When the space of sequence number is exhausted, the sender and the receiver enter the re-authentication stage go renew the session key and reset the counter.

III. PROPOSED SCHEME

The proposed security scheme is designed to provide a lightweight identity authentication at the link layer for data frame in WSNs. The main idea is to generate a chain for authentication in the base station and the sensor node, and then only add n -bits from this chain into the MAC-layer data frame for identity authentication. Unlike traditional authentication scheme, the proposed scheme determines the legitimacy of a sender by continuously checking a series of data frames transmitted by the sender. The goals of our lightweight authentication scheme are the following:

- **Secure and Useful:** an attack node should with low probability be able to success attack to the network.
- **Cheap:** by presenting an optimized n -bits identity authentication method for resource-constrained environments like wireless sensor networks, a cheap and efficient access control procedure is obtained.
- **Robust:** due to loss channels in wireless communications a synchronization algorithm is required for the generated authentication chain in the base station and the sensor node.
- **Per-Frame Authentication:** the protocols should authentication the sender continuously, i.e., for each transmitted packet.

Also, the following assumptions are considered in the design of the protocols:

- a) Shared key between base station and sensor node should be provided by the key distribution mechanism, but are out of scope of this paper.

b) Wireless communication is not secure; it is broadcast and any adversary can eavesdrop, replay, or inject messages.

c) Schemes do not place any trust assumption on the communication infrastructure. Frames might not be delivered to the receiver. This is an essential part of the authentication protocol and the reason for the synchronization schemes.

In this paper, the following notations are used to describe the proposed scheme:

Notation	Description
B, N	Base Station(B , Receiver), Sensor Node(N , Sender)
ASG	Authbit Sets Generator
SNG	Set Numbers Generator
ASC	Authbit Sets Chain
$\{S\}_{BN}$	L -bits stream shared between B and N
$SP(k)$	Set pointer which indicate the k^{th} set of ASC
$\{Authbit\}_{SP(k)}$	n -bits authentication value which is indicated by $SP(k)$

Ideally, since the attacker does not have the shared key, the probability for the attacker to guess continuously i times of n -bits is as small as $(2^n)^{-i}$. In Figure 1, the operation of proposed authentication scheme is shown, in which the left part of the figure describe the base station (receiver) operation and the right part describe the sensor node (sender) operation.

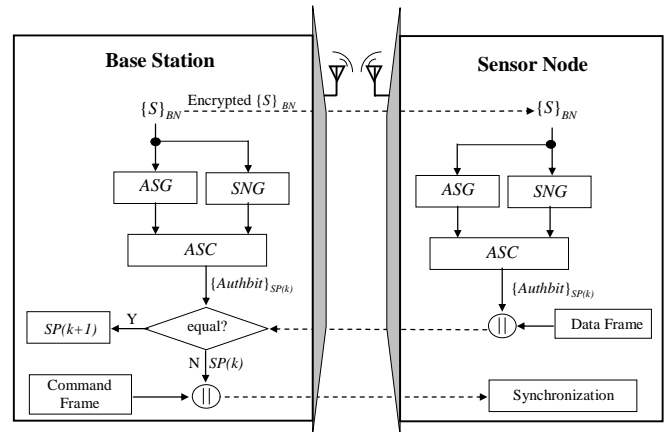


Figure 1. The operation of proposed scheme

A. Authbit set and Set number

If the base station (B) determines acceptance of sensor node (N), encrypted L -bits $\{S\}_{BN}$ (as shown in Figure 2) will be transmitted to node by base station within association process. In other word, base station and sensor node have the same L -bits $\{S\}_{BN}$ using the secure transmission.

a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
1	0	0	1	1	1	0	1
a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}
1	0	0	1	0	0	1	1

Figure 2. The example of L -bits $\{S\}_{BN}$ (where $L=16$)

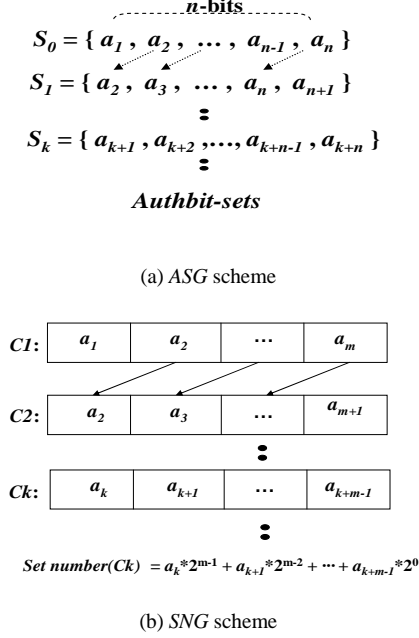


Figure 3. (a) Authbit sets and (b) Set numbers generation scheme

And then, the base station and the sensor node create *Authbit sets* and *Set numbers* using the (a) ASG and (b) SNG scheme (as shown in Figure 3). For example, if the base station and the sensor node use the $\{S\}_{BN}$ of Figure 2, $S_0=\{1,0,0\}$, $S_1=\{0,0,1\}$ and $S_2=\{0,1,1\}$ where $n=3$. Also, $C1=a_1*2^3+a_2*2^2+a_3*2^1+a_4*2^0=9$ and $C2=3$, and $C3=7$ where $2^m = L = 16$. Finally, the *Authbit set* and the *Set number* will be used making the same chain for authentication of data frame between the base station and the sensor node as shown in Figure 4.

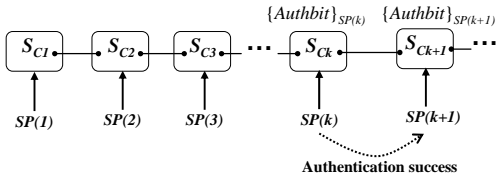


Figure 4. ASC (*Authbit Sets Chain*) scheme

In the Figure 4, if the base station and the sensor node use the $\{S\}_{BN}$ of Figure 2 (where $n=3$), the first component of authentication chain will be set $S_0 = \{0,0,1\}$ and the second component will be set $S_3 = \{1,1,1\}$. Also the third component will be set $S_7 = \{1,1,0\}$.

B. Synchronization and Fault Tolerance using the Set Pointer

Conceptually, both the base station and the sensor node have a pointer pointing to the $\{Authbit\}_{SP(k)}$ for the next outgoing data frame (as shown in Figure 4). Ideally, both the base station and the node will have their pointer pointing at exactly the same $\{Authbit\}_{SP(k)}$ and advance synchronously. Initially, the base station and the node pointers are synchronized as $SP(1)$. The sensor node sends each data frame with n -bits and bits value is equal to the values of the $SP(k)$. When the base station receives a frame successfully, the base station checks the bits value of the data frame. The synchronization and fault tolerance of $SP(k)$ can partially be described with the Figure 4 and Figure 5. Let the number of synchronization done by node and base station be s .

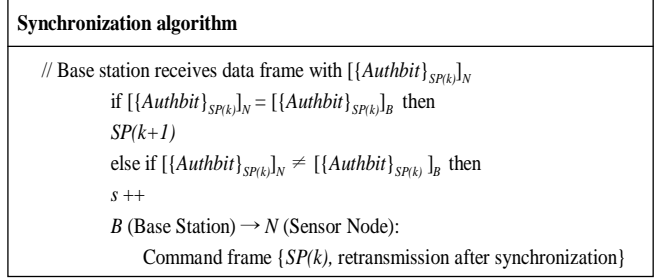


Figure 5. Pseudo code of synchronization algorithm

IV. STATISTICAL METHOD AND SIMULATION

The main objective of this authentication scheme is to determine whether the sending node is an attacker or not. If the $\{Authbit\}_{SP(k)}_N$ doesn't match the $\{Authbit\}_{SP(k)}_B$, this means there are two possibilities either (a) there is no synchronization between the base station and the sensor node $SP(k)$ or (b) the sending node is an illegitimate node. In an error-prone wireless network, data frames are 'frequently' lost due to wireless error. In [4], authors proposed a lightweight authentication protocol for access control in WLAN. They have devised a statistical method to determine the probability of a station being an attacker. We expanded the statistical method of their paper to support to our proposed scheme. We know that in a perfect channel, where there are no losses, a legitimate node will not have any synchronization with its receiver. However, in an error-prone wireless network, a receiver (base station) cannot differentiate between non-synchronization due to attacker and non-synchronization due to wireless losses. Hence, we devise a statistical method to determine the probability of a sending node being an attacker. Let the number of data frames from $SP(1)$ to $SP(t)$ be t , let the number of synchronization done by node and base station be s , and let the data frame loss rate be r , where r ($0 \leq r \leq 1$). We have the following theorem.

A. Theorem (where using n -bits authentication stream)

For a sending node D , assume the prior probability of node D to be an attacker is $\frac{1}{2^n}$, i.e., $P(D=\text{attacker}) = \frac{1}{2^n}$ and

$P(D=\text{legitimate}) = \frac{2^n - 1}{2^n}$, the probability of this node D being an attacker is one when the number of synchronization is s , $P(D=\text{attacker} | t, s)$, is given by

$$P(D=\text{attacker} | t, s) = \frac{2^{-t}}{2^{-t} + (2^n - 1) * r^s (1-r)^{t-s}} \quad (1)$$

B. Proof

We know $P(D=\text{legitimate} | t, s) = 1 - P(D=\text{attacker} | t, s)$.

According to Bayer's Formula, we have

$$P(D=\text{attacker} | t, s) = \frac{P(t, s | D = \text{attac ker}) * P(D = \text{attac ker})}{P(t, s | D = \text{attac ker}) * P(D = \text{attac ker}) + P(t, s | D = \text{legitimate}) * P(D = \text{legitimate})}$$

$$= \frac{P(t, s | D = \text{attac ker})}{P(t, s | D = \text{attac ker}) + (2^n - 1) * P(t, s | D = \text{legitimate})} \quad (2)$$

First let us assume that the sending node is an attacker; also it does not know the ASC. In this case, the probability of

$P(t, s | D=\text{attacker})$ can be given as follows:

$$P(t, s | D=\text{attacker}) = \binom{t}{s} * 2^{-t} \quad (3)$$

Now let us consider the case where the sending node is a legitimate node. We have the probability of the number of synchronization s where the data frame loss rate is r :

$$P(t, s | D=\text{legitimate}) = \binom{t}{s} * r^s (1-r)^{t-s} \quad (4)$$

Combing (2), (3) and (4), it is easy to derive (1), i.e.,

$$P(D=\text{attacker} | t, s) = \frac{2^{-t}}{2^{-t} + (2^n - 1) * r^s (1-r)^{t-s}}$$

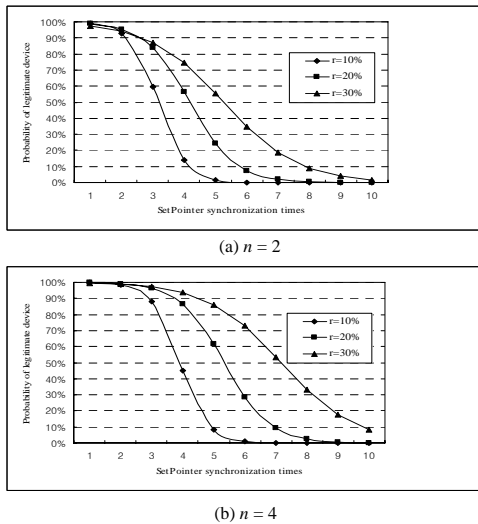


Figure 6. Probability of legitimate sender where $n=2$ and $n=4$

Figure 6 shows the probability of a sending node being a legitimate one. We have $t=10$. The analysis is for $r=10\%$, 20% and 30% . As shown in Figure 6(a), in case of the data frame loss rate is 10% in wireless sensor network; if the synchronization has been happen three times ($s=3$), the probability of sending node being a legitimate one is near 60% . If the synchronization has been four times ($s=4$), however, the probability values lower than 20% . Therefore, we can decide a level of reliance and then detect the attack according to the probability values.

Figure 7 shows the probability of a sending node being a legitimate one. We have $t=10$. The analysis is for $n=2, 3$ and 4 .

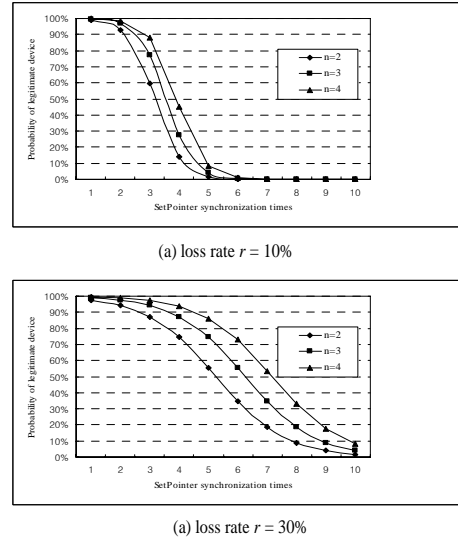


Figure 7. Probability of legitimate sender where $r=10\%$ and $r=30\%$

Also, Figure 8 shows a frame sequence chart from association request to frame identity authentication between base station and sensor node by using the proposed ASC to authenticate each other.

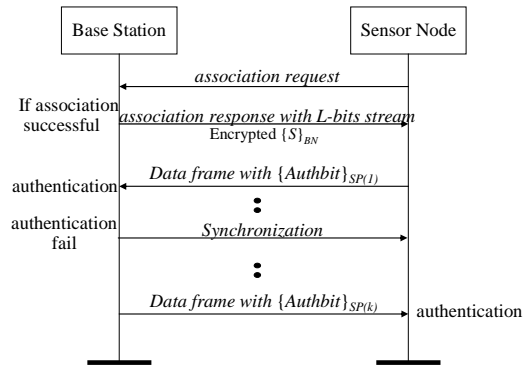


Figure 8. Frame sequence chart with ASC

V. CONCLUSION

In this paper, we have presented a lightweight identity authentication scheme for data frame in wireless sensor networks. The proposed scheme inserts identity authentication

bits from a data frame known only to the two communicating nodes. With the proposed scheme there are only n -bits for identity authentication, which can greatly reduce overhead and thus preserves the scarce wireless bandwidth resource. The major purpose of the proposed scheme is to detect an attack in an error-prone wireless environment. When the coordinator detects an attack, some protection or anti-attack approaches for each type attack can be triggered. We plan to foster our solution in the evolutionary computing systems through further development.

REFERENCES

- [1] "Wireless Medium Access Control and Physical Layer Specification for Low-Rate Wireless Personal Area Networks", IEEE Standard, 802.15.4-2003, May 2003.
- [2] N. Sastry, D. Wagner, "Security Consideration for IEEE 802.15.4 Networks", WiSe'04, Proceeding, pp.32-42, 2004.
- [3] Henric Johnson, Arne Nilsson, Judy Fu, S.Felix Wu, Albert Chen and He Huang, "SOLA: A One-bit Identity Authentication Protocol for Access Control in IEEE 802.11", In Proceedings of IEEE GLOBECOM 2002.
- [4] Haoli Wang, Aravind Velayuthan, Yong Guan, "A Lightweight Authentication Protocol for Access Control in IEEE 802.11", In Proceedings of IEEE GLOBECOM 2003.
- [5] Fan Zhao, Yongjoo Shin, S. Felix Wu, Henric Johnson, Arne Nilsson, "RBWA: An Efficient Random-Bit Window-based Authentication Protocol", In Proceedings of IEEE GLOBECOM 2003.
- [6] Jose A. Gutierrez, Edgar H. Callaway Jr, Raymond L. Barrett Jr, "Low-Rate Wireless Personal Area Networks", IEEE Std 802.15.4.
- [7] Mohammad Ilyas, Imad Mahgoub, "Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems" CRC PRESS, 2004.
- [8] J.R. Douceur, "The sybil attack", In IPTPS, pp.215-260, 2002.
- [9] Agah. Afrand, Das, S.K., Basu, K.," A game theory based approach for security in wireless sensor networks", Performance, Computing, and Communications, 2004, pp. 259 – 263.
- [10] A. Menezes, P. Oorschot, S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1997.
- [11] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J.D.Tygar, "SPINS: Security protocols for sensor networks," Proceedings of MOBICOM 2001.
- [12] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, "System architecture directions for networked sensors," Proceedings of the 9th International Conference on Architectural Support for Programming Languages and Operating Systems, November 2000.