ICOIN 2015, Jan 12-15, 2015, Cambodia

Secured Node-to-Node Key Agreement for Wireless Sensor Networks

Jaruwan Mesit
Department of Computer Science
Grambling State University
Grambling, USA
Email: mesitj@gram.edu

Matthias R. Brust
College of Engineering and Science
Louisiana Tech University
Ruston, USA
Email: mbrust@latech.edu

***Abstract*—Sensor networks are mostly deployed in unsecured environments, thus protecting a sensor network from any attack is critical in order to maintain the health of the network. Recently, many researchers have focused on making security for sensor networks available and reliable. In this paper, a secured node-to-node key agreement protocol is proposed to generate secured communication among principle nodes A and B, a ticket granting server, and a key server.**

Since a sensor network is usually a resource-constrained infrastructure, it is not suitable for computationally expensive asymmetric key protocols such as public-private key cryptography. Therefore, setting up a shared key in our proposed protocol is based on a symmetric key protocol processed by two trusted agents, which are the ticket granting server and the key server. The data confidentiality, authentication, and freshness of the network security are also considered in the design of the proposed protocol.

***Index Terms*—Wireless sensor networks; Security; Authentication; Confidential; Freshness**

I. Introduction

Wireless sensor networks (WSN) have been identified as one of the most incredible technologies for many applications such as tank movement, ship arrivals and departures, etc. [1][2], [3]. For each area of wireless sensor networks, a cluster of sensor nodes is deployed to collect the data that is later reported to the network base station [4]. To collect the data in such a network, the sensor nodes can relay the data to the base station.

A wireless sensor network can be considered as a highly intensive data collector. This means that the security of data transfer and access become critical issues. Three well-known security goals are: only authorized user can access the data (confidentiality), the data should be genuine (integrity), and the data should be available for the authorized user (availability) [5]. All these goals are the requirements from both users and wireless sensor networks.

Possible attacks in wireless sensor networks include physical destruction of sensor nodes, security attacks on the routing and data link protocols, and resource consumption attacks. Unattended sensor node deployment can cause another attack in which an adversary may try to compromise several sensor nodes and inject false data into the network through the compromised sensor nodes.

In this paper, a secured node-to-node key agreement is proposed to ensure that only an authorized user can access the network, and so that it is ensured that data is only available for the authorized user.

The structure of this paper is organized as follows. Section II describes the related work. Section III explains the implementation of the proposed protocol and Section IV concludes the work of this paper.

II. Related Work

Related work that focuses on the security issues in computer networks is presented here.

In [6], Fox and Gribble described the security and authentication on open networks. This protocol provides lightweight secured communication at the client module using the interaction with a proxy to Kerberos [7] at the application-level proxy service.

In [8], Patel and Crowcroft provided the security in mobile user where asymmetric cryptography has been used with a ticket-based service access model allowing anonymous service usage in mobile application. The mobile users anonymously contact the credential center to check for the user's certification for the access. However, the asymmetric cryptography is cost-inefficient for a sensor network environment.

In [9], Perrig et al. presented a security protocol for multicast communication. The paper focused on securing multicast communication at the source authentication and enabling receivers of multicast data to ensure that the received data is originated from the source. The paper proposed the modification to TESLA (Timed Efficient Stream Loss-tolerant Authentication) to allow receivers to authenticate the packets when they arrive. TESLA implements a loose time synchronization between the sender and the receivers, followed by delayed release of keys by the sender.

In [10], Liu and Ning presented the broadcast authentication in distributed sensor networks where the development of a scalable broadcast authentication scheme named multilevel μTESLA based on the original μTESLA protocol [11]. Multilevel μTESLA provided several improvement which included low overhead, tolerance of message loss, scalability to large networks, resistance to replay attacks, and denial-of-service attacks (DoS).

In [12], Ren et al. claimed that both μTESLA and multilevel μTESLA suffered from serious DoS attacks due to the delay of

Step	Key Agreement
1	$A \rightarrow B : N_{A_1}, A$
2	$B \rightarrow T : N_{A_1}, N_{B_1}, A, B, MAC\left(K_B, N_{A_1} \vert N_{B_1} \vert A \vert B\right)$
3	$T \rightarrow A : \{K_{TSA}\}_{k_A}, MAC\left(K'_{TSA} \vert N_{A_1} \vert A \vert B \vert \{T_n \vert K_{TSA}\}_{k_A}\right)$
4	$T \rightarrow B : \{K_{TSB}\}_{k_B}, MAC\left(K'_{TSB} \vert N_{B_1} \vert A \vert B \vert \{T_n \vert K_{TSB}\}_{k_B}\right)$
5	$A \rightarrow S : N_{A_2}, A, B, MAC\left(K'_{TSA} \vert N_{A_2} \vert A \vert B \vert \{T_n\}_{k_{TSA}}\right)$
6	$B \rightarrow S : N_{B_2}, A, B, MAC\left(K'_{TSB} \vert N_{B_2} \vert A \vert B \vert \{T_n\}_{k_{TSB}}\right)$
7	$S \rightarrow A : \{K_{AB}\}_{k_A}, MAC\left(K'_A \vert N_{A_2} \vert A \vert B \vert \{K_{AB}\}_{k_A}\right)$
8	$S \rightarrow B : \{K_{AB}\}_{k_B}, MAC\left(K'_B \vert N_{B_1} \vert A \vert B \vert \{K_{AB}\}_{k_B}\right)$

Figure 1. The eight steps of the key agreement.

message authentication. They used the public key concept to achieve the broadcast authentication. Cryptographic techniques includes Merkle hash tree and identity-based signature scheme have been adopted to minimize the costs on computation and communication in wireless sensor networks.

In [13], Sultana et al. focused on malicious packet dropping attack in the sensor network. They proposed a data provenance based mechanism to detect the attack and identify the malicious node. The proposed scheme based on the watermarking based secure provenance transmission. The scheme includes packet loss detection, identification of attack presence, and localizing the malicious node/link.

In [14], Oliveira et al. used Pairing-Based Cryptography (PBC) protocols for key distribution in wireless sensor networks. The concept of Pairing-based Cryptography (PBC) protocols is that the parties can agree on keys without any interaction. The TinyPBC presented in this paper was able to compute pairings, the most expensive primitive of PBC for 8, 16 and 32-bit processors sensor nodes.

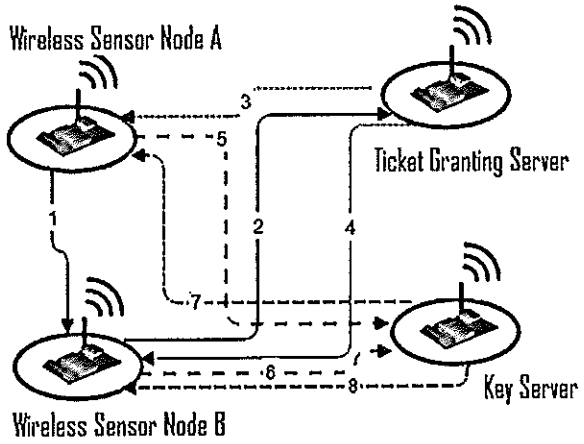

Figure 2. Illustration of the steps of the proposed node-to-node key agreement.

III. Implementation

In order for nodes to communicate in a wireless sensor network, a node-to-node key agreement has to be established. This key agreement provides security of the communication, which includes authentication, availability, and freshness. As mentioned in [11], due to the resource-constrained sensor nodes, the computationally expensive public-key cryptography is not suitable. Therefore, the protocol for symmetric-key is suggested.

For the purpose of gaining stronger freshness, the two trusted agents, key server S and the ticket granting server T, are included in our proposed protocol for the node-to-node key agreement. A message authentication code (MAC) is additionally used for two-party authentication and data integrity.

The following notations are used in this paper.

A, B	are principles, such as communication nodes
$N_{A_1}, N_{A_2}, N_{B_1}, N_{B_2}$	are Nonce numbers from A and B
$M_1 \vert M_2$	denotes the concatenation of message M_1 and M_2
K_A	is the key of node A shared with base station
K_{AB}	is the pairwise key shared between nodes A and B
K_{TSA}	is the shared key between nodes T, S, and A
$\{M\}_{k_{TSA}}$	is the encrypted message with the symmetric key K_{TSA}
T_n	is the ticket number to communicate with T
MAC	is the message authentication code

The proposed node-to-node key agreement provides secured key agreement and stronger key freshness. The steps of the key agreement are given in Fig. 1 and illustrated in Fig. 2.

The detail of each step of the proposed method is explained here. We start from step 1 when the wireless sensor node A would like to communicate with node B. Node A sends a request to node B with nonce number N_{A_1}. In step 2 node B sends N_{B_1} with a request for a ticket from ticket granting

server T. This ticket is used for communication between node A and B, and the key server S. In steps 3 and 4, the ticket granting server T grants a ticket and sends to nodes A and B.

The messages sent from the ticket granting server T to nodes A and B are encrypted with key K_A and key K_B, respectively. Then in steps 5 and 6, nodes A and B send the ticket to the key server S to ask for the shared key K_{AB}. At these steps, nodes A and B sends the messages to the key server with the nonce numbers N_{A_2} andN_{B_2} respectively. As mentioned earlier, the nonce numbers provide the freshness of the communication. The key server S receives the ticket and then issues the shared key K_{AB} to nodes A and B in steps 7 and 8.

For the confidentiality, all messages sent from either the ticket granting server T or the key server S to nodes A or B are encrypted by K_A or K_B. Thus only node A or node B can decrypt the messages. All these messages are authenticated with MAC protocol. Thus the proposed method provides the three properties of wireless sensor security for node-to-node key agreement; all of which are freshness, confidential, and authentication.

IV. Conclusion

The proposed method presents the node to node key agreement which is provided by the ticket granting server T and the key server S. There are several steps to set up a shared key for nodes A and B to securely communicate. Starting from node A sends a request to node B. Node B receives the request and asks for a ticket from the ticket granting server T. This ticket is required for nodes A and B to communicate with the key server S. After the ticket is granted to nodes A and B, nodes A and B send this ticket to the key server S. The key server S issues the shared key to nodes A and B. Finally nodes A and B can communicate with each other using the shared key.

The authentication, confidential, and freshness of the secured communication are efficiently achieved by this proposed method, as the proposed protocol uses the MAC to authenticate the messages, the shared key to communicate between nodes A and B, and the nonce numbers to refresh the messages.

References

[1] M. İ. Akbaş, M. R. Brust, and D. Turgut, "Sofrop: Self-organizing and fair routing protocol for wireless networks with mobile sensors and stationary actors," *Computer Communications*, vol. 34, no. 18, pp. 2135–2146, 2011.

[2] M. R. Brust, M. İ. Akbaş, and D. Turgut, "Multi-hop localization system for environmental monitoring in wireless sensor and actor networks," *Wiley Journal on Concurrency and Computation: Practice and Experience*, vol. 25, no. 5, pp. 701–717, 2011.

[3] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, pp. 2292–2330, Aug. 2008.

[4] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "Interleaved hop-by-hop authentication against false data injection attacks in sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 3, no. 3, p. 14, 2007.

[5] Z. Benenson, P. M. Cholewinski, and F. C. Freiling, "Vulnerabilities and attacks in wireless sensor networks," *Wireless Sensors Networks Security, Cryptology & Information Security Series (CIS)*, pp. 22–43, 2008.

[6] A. Fox and S. D. Gribble, "Security on the move: indirect authentication using kerberos," in *Proceedings of the 2nd annual international conference on Mobile computing and networking*, pp. 155–164, ACM, 1996.

[7] B. C. Neuman and T. Ts'o, "Kerberos: An authentication service for computer networks," *Communications Magazine, IEEE*, vol. 32, no. 9, pp. 33–38, 1994.

[8] B. Patel and J. Crowcroft, "Ticket based service access for the mobile user," in *Proceedings of the 3rd annual ACM/IEEE international conference on Mobile computing and networking*, pp. 223–233, ACM, 1997.

[9] A. Perrig, R. Canetti, D. Song, and J. Tygar, "Efficient and secure source authentication for multicast," in *Network and Distributed System Security Symposium, NDSS*, vol. 1, pp. 35–46, 2001.

[10] D. Liu and P. Ning, "Multilevel μtesla: Broadcast authentication for distributed sensor networks," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 3, no. 4, pp. 800–836, 2004.

[11] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. E. Culler, "Spins: Security protocols for sensor networks," *Wireless networks*, vol. 8, no. 5, pp. 521–534, 2002.

[12] K. Ren, W. Lou, K. Zeng, and P. J. Moran, "On broadcast authentication in wireless sensor networks," *Wireless Communications, IEEE Transactions on*, vol. 6, no. 11, pp. 4136–4144, 2007.

[13] S. Sultana, E. Bertino, and M. Shehab, "A provenance based mechanism to identify malicious packet dropping adversaries in sensor networks," in *Distributed Computing Systems Workshops (ICDCSW), 2011 31st International Conference on*, pp. 332–338, IEEE, 2011.

[14] L. B. Oliveira, D. F. Aranha, C. P. Gouvêa, M. Scott, D. F. Câmara, J. López, and R. Dahab, "Tinypbc: Pairings for authenticated identity-based non-interactive key distribution in sensor networks," *Computer Communications*, vol. 34, no. 3, pp. 485–493, 2011.