WMNC 2015, Oct 5-7, 2015, Germany

Securely Create Public Keys and Private Keys for Sensor Networks

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

Abstract—**Due to the potentially unsecured environment of a wireless sensor network, protecting it from any attack is significant importance to maintain the health of the network. Recently, many researchers have focused on providing the security on making sensor networks available and reliable for the nodes to communicate to each other.**

In this paper, we propose a secure and efficient method for node to node key agreement in unsecured wireless sensor networks. The main idea of the proposed key agreement is to use a ticketing grant server and a key server to generate a shared key for the principal nodes to communicate in the wireless sensor network environment. To create the secure environment, two cryptography protocols take into our consideration, symmetric ciphers such as shared key encryption and asymmetric ciphers such as public-private key encryption. Wireless sensor networks are resource-constrained environments, which are improper for computationally expensive that occurs in public-private key encryption. Therefore, the key in our protocol is solely based on a symmetric protocol provided by two trusted agents, the ticketing grant server and the key server. A ticketing server is to provide a ticket for the principal nodes to communicate with the key server. Then the key server generates a shared key that principal nodes can use to secure the communication between each other. The confidentiality, authentication, and freshness of the network security are discussed to analyze the performance of our proposed method.

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

I. Introduction

Wireless sensor networks (WSN) are composed of a potentially large set of devices that communicate over a wireless medium. Such networks can be formed spontaneously whenever devices are in communication or transmission range. Joining and leaving of nodes occurs dynamically, particularly in the presence of mobility (e.g., vehicular sensor networks). Two mobile devices out of communication range can use intermediary devices for relaying packets. 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 [1]. To collect the data in such a network, the sensor nodes can relay the data to the base station. Although, many advantages are in favor of the use of wireless sensor networks, they also suffer from limited battery lifetime, interference, noise and—in particular—security. Potential applications of wireless sensor networks can be found in traffic scenarios, vehicular ad hoc and sensor networks, ubiquitous Internet access, and collaborative work [2], [3], [4].

Due to the nature of these applications which always broadcasts the radio transmission from the sensor nodes to the base station, the wireless sensor network is more vulnerable to network attacks than other traditional networks. In order to protect the sensor nodes from the attacks, the implementation of cryptography becomes more important to achieve the objectives of network security. Several topics of cryptography have been well studied for traditional networks. However, many conventional cryptographic approaches cannot be appropriately applied to the wireless sensor networks. For the implementation analysis, public-private key schemes and some symmetric key methods are still too complicated for the wireless sensor networks in the terms of computations, memory, communications, and packet size requirements. In addition, wireless sensor networks suffer from some other severe constraints on the network resources which refer to the necessity of increasing the network lifetime, minimizing the physical size of the sensor nodes, and reducing the cost of sensor nodes.

A wireless sensor network can be considered as highly intensive data collection (i.e., meaning that the security of data transfer and access becomes critical issues). Three well known security goals are: only authorized user can access to 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.

A possible attack scenario in wireless sensor networks includes 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 it is ensured that data is only available for the authorized user. The key in our protocol is solely based on a symmetric protocol provided by two trusted agents, the ticketing grant server and the key server. The proposed

protocol is less complex compared to the other protocols that apply asymmetric encryption scheme with regards to the computation, memory usage, and packet size requirements.

The structure of this paper is organized as follows. Section II describes the related work. Section III explains the implementation of the proposed protocol; Section IV presents a performance comparison with existing methods and provides a complexity analysis and Section VI 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 message authentication. They used the public key concept to achieve the broadcast authentication. Cryptographic techniques including 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.

III. Implementation

A. Routing protocol

The routing protocol that we have chosen for this paper is SOFROP (Self-Organizing and Fair ROuting Protocol) [4], [15]. This protocol is efficient and provides the lightweight routing that is optimized for fairness and the locally acting adaptive overlay network formation. SOFROP is a routing protocol capable of dealing with an unpredictable environment with a diversity of mobility elements. On the network organization level, it is able to continuously adapt the sensor network topology and deal with challenges such as rapid changes in the link structure. The protocol is proven to provide an efficient bandwidth utilization and data transmission, which are important aspects for the settings used in this paper.

SOFROP considers a topology control layer, which determines dedicated nodes to be the *cluster heads* (or *routing nodes*). These routing nodes form a backbone network on a otherwise flat network topology. The routing nodes election process can be implemented by using heuristics [16] or a multi-hop hierarchical clustering structure (e.g., applying the multi-hop clustering algorithm KHOPCA [17]).

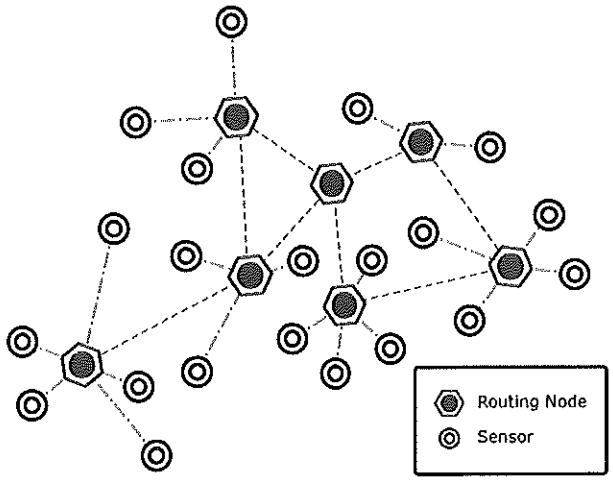

Figure 2. Wireless sensor nodes and routing nodes.

B. Node-to-node key agreement

After SOFROP identifies the next sensor node, the identified node needs to communicate with the previous node along the communication path. This means node-to-node key

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.

agreement has to be established. The proposed key agreement in this paper provides the security of the communication which includes authentication, availability, and freshness. Two cryptography protocols take into our consideration. The former protocol is symmetric ciphers such as shared key encryption. This symmetric ciphers require one public key generated for the communication between nodes. The latter protocol is asymmetric ciphers such as public-private key encryption. This asymmetric ciphers required two different key generated.

As mentioned in [11], due to the resource-constrained in the sensor nodes, the computationally expensive public-private key cryptography in asymmetric ciphers is not suitable. Therefore, the protocol for symmetric-key is suggested.

In addition for the purpose of gaining stronger freshness, the nounce numbers are used for the communication between the principal nodes and the two trusted agents, key server S and the ticket granting server T. A message authentication code (MAC) is additionally used for two-party authentication and data integrity.

For the node-to-node key agreement description, we use the following notations 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
K_{TSA}	is the shred key between nodes A and B
MAC	is the message authentication code

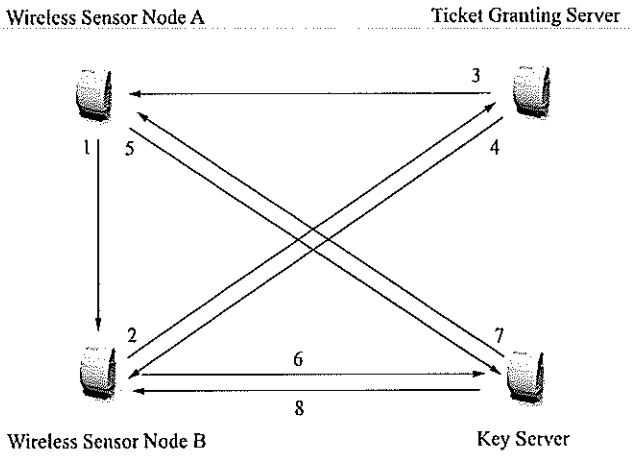

Figure 3. Illustration of the steps of the proposed node-to-node key agreement.

The proposed node-to-node key agreement provides secured key agreement and stronger key freshness. The step of the key agreement is as follows:

In our key agreement $N_{A_1}, N_{A_2}, N_{B_1}$ and N_{B_2} that produced by node A and B guarantee the freshness of the communication between principle nodes A and B, ticket granting server 1 and the key server S. The security is increased by not only for connecting to the key server but also to the ticket granting server. To provide the confidentiality, the key K_{TAB} is used for the communication between nodes A and B. This ticket is authenticated with the message 3authentication code MAC.

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.

C. MAC Authentication

MAC Authentication is a cryptographic technique that computes checksum on data. This cryptography uses a session key to detect both accidental and intentional modifications of the data. Two inputs, a message and a secret key that is known by only the original sender and its intended recipient, are required for a MAC authentication. This cryptography allows the recipient to verify the integrity of the message and to authenticate the message as only the original sender and its intended recipient have the shared secret key. In case the sender is an attacker who does not know the secret key, the value that is returned form the hash function would be different and that would notify to the recipient that the message was not sent by the original sender. On another hand, if the attacker pretends to be the recipient who does not know the secret key, then the message will not be read by the pretending recipient.

Four types of MACs can be selected; all of which are unconditionally secure, hash function-based, stream cipher-based and block cipher-based. The most common approach to creating a MAC that was common used in the past was the block ciphers such as Data Encryption Standard (DES). However hash-based MACs (HMACs) that apply a secret key in conjunction with a cryptographic hash function to produce a hash, have become more widely used and is used in the proposed scheme.

IV. Comparison and Computation Analysis

To evaluate and compare the performance of the proposed key agreement scheme with the existing schemes for wireless sensor networks, the complexity of communication and procession operations is the important metric. In this manner, our proposed key agreement scheme has some advantages over the existing public and private key schemes. With this proposed method, the high cost public-key encryption has been replaced by symmetric encryption at the sensor nodes with the hash function at the MAC authentication. In addition, to establish node-to–node key agreement, only four local nodes are communicated to each other.

For the communication overhead of the proposed protocol, the sensor nodes, ticket server, and key server collaborate with each other to produce an exclusive node-to-node key for each communication. However, with this process the computation of ticket and key generations are required at the ticket server and key server, respectively. According to this operation for each communication between nodes requires the key establishment process that will be perform at the ticket server and then key server. Let n be the number of sensor nodes. On the average there are $\frac{n}{2}$ communications for node-to-node key generation. Each communication requires one ticket and one session key which means over all the computation of this method is approximately $2\frac{2}{n}$.

V. Performance Analysis and Discussion

The first question is how this protocol can provide freshness of the secure communication. The freshness of this protocol is from using the nonce numbers that are generate at the steps 1, 2, 5, and 6. When node A sends the request to node B, node A sends the request with the nonce number N_{A_1} and then node B communicates with the ticket granting server by sending its nonce number N_{B_1} along with the node's A nonce number. This is to guarantee that the communication is fresh and it is a newly established communication. When nodes A and B communicate with the key server S, nodes A and B regenerate the nonce numbers N_{A_2} and N_{B_2}. The nonce number regeneration is for the purpose to provide freshness to the communication with the key server S.

The second question is how this protocol can provide confidential. When the ticket granting server T communicates with node A, the ticket granting server uses node's A key, K_A, to encrypt the message. Only node A can decrypt the message. Similar to communicate with node B, the ticket granting server T uses node's B key, K_B, to encrypt the message. Only node B can decrypt the message. Then nodes A and B communicate with the key sever S, the message sent from nodes A and B are encrypted by the key server's keys, K_{TSA}, for the message sent by A and for the message sent by B; only the key server S can decrypt the message. Then the shared key, K_{AB} , is sent to nodes A and B being encrypted by node's A key, K_A, and node's B key, K_B; only nodes A and B can decrypt the message.

Finally, the last question is how this protocol can provide authentication. The protocol is authenticated by Message Authentication Code MAC which is used at steps 2 to 8. This cryptography uses a session key to detect both accidental and intentional modifications of the data. This can be achieved by using Cipher Block Chaining Message Authentication Code [?]. Two inputs, a message and a secret key that is known by only the originator its intended recipient(s), are required for a MAC authentication. The recipient can verify and authenticate the integrity of the message as only the sender has the shared secret key.

VI. 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. This request is sent to node B along with the nounce number N_{A_1}. Node B receives the request from node$A$ and asks for a ticket from the ticket granting server T. The request for the ticket is sent to ticket granting server T with nounce numbers N_{A_1} and N_{B_1}. 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 generate new nounce number N_{A_2} and N_{B_2} and send the new nounce numbers with the 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.

In future work, we plan to focus on the key generation characteristics for the reason that a more efficient and scalable key generation can be achieved by considering the keys among the neighboring nodes. Additionally, further future work includes the problem of how the ticket can be generated at the ticket granting server T and how the shared key can be provided using criteria and the environment of the wireless sensor networks.

References

[1] 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.

[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] 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.

[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.

[15] M. I. Akbas, M. R. Brust, and D. Turgut, "SOFROP: Self-Organizing and Fair Routing Protocol for Wireless Networks with Mobile Sensors and Stationary Actors," in *Proceedings of the IEEE Conference on Local Computer Networks (LCN)*, pp. 464–471, 2010.

[16] M. R. Brust, A. Andronache, S. Rothkugel, and Z. Benenson, "Topology-based Clusterhead Candidate Selection in Wireless Ad-hoc and Sensor Networks," in *2nd International Workshop on Software for Sensor Networks (SENSORWARE 2007)*, (Bangalore, India), p. 8, 2007.

[17] M. R. Brust, H. Frey, and S. Rothkugel, "Dynamic Multi-Hop Clustering for Mobile Hybrid Wireless Networks," in *Proceedings of the Second International Conference on Ubiquitous Information Management and Communication (ACM ICUIMC 2008)*, (Suwon, Korea), pp. 130–135, ACM Press, 2008.