

DoS-Resilient Authenticated Key Agreement Scheme between Actor and Sensor nodes in Wireless Sensor and Actor Network

Imsung Choi, Zeen Kim and Kwangjo Kim

Korea Advanced Institute of Science and Technology
{theshaki, zeenkim, kkj}@kaist.ac.kr

Abstract. In this paper, we address the Authenticated Key Agreement (AKA) between actor and sensor nodes in Wireless Sensor and Actor Network (WSAN). We propose DoS-resilient AKA scheme between Actor and Sensor nodes in WSAN. The proposed scheme utilizes the ID-based cryptosystem to reduce a need to transmit public-key certificates. The proposed scheme is resilient against the Denial of Service (DoS) attacks which are identified in [13] by using the geographic information of sensor nodes as their identity information. The proposed scheme also considers the asymmetric resources of actor and sensor nodes. We then analyze the security of the proposed scheme and then discuss the performance of the proposed scheme.

1 Introduction

Recently, Wireless Sensor and Actor Network (WSAN), which is the integration of Mobile Ad-hoc Network (MANET) that consists of mobile nodes and Wireless Sensor Network (WSN) that consists of a number of resource-limited sensor nodes, has merged [1]. Because of the coexistence of actor and sensor nodes, the conventional schemes for both MANET and WSN cannot be applied directly to WSAN. So far, many issues in WSAN have wide attention, but the security issue has less attention.

Security support is a must for WSAN in some environments such as tactical environments or commercial environments. Conventional security schemes [7, 8] of WSN which are based on probabilistic approach are not suitable for WSAN because they are not scalable (*i.e.*, when the size of network increases, the size of keys to store also increases). Therefore, for the security of WSAN, Authenticated Key Agreement (AKA) is one of the promising mechanisms to build a secure network.

A few schemes [11, 12] addressed the AKA problem of WSAN, but these schemes have some weaknesses in AKA between sensor and actor nodes. Cao *et al.*'s scheme [12] utilized a symmetric key which is shared by all nodes for AKA between actor and sensor nodes. In this scheme, the actor nodes cannot perform AKA scheme dynamically because all nodes remove the key after first AKA, even though actor nodes generally require to communicate dynamically with sensor

nodes [5, 6]. For additional AKA, the Base Station (BS) should distribute a new key to all nodes. If the topology changes frequently, it causes a big communication overhead. Yu *et al.*'s scheme [11] utilized the public key cryptosystem for AKA between actor and sensor nodes, but it needs a big overhead for sensor nodes to transmit public-key certificates and to perform public key encryption and decryption. Yu *et al.*'s scheme [11] also does not support the key agreement. Instead, the sensor node just chooses a random number as the session key.

In this paper, we propose the AKA scheme for actor and sensor nodes in WSN. The proposed scheme utilized the ID-based cryptosystem to reduce a need to transmit public-key certificates. In the proposed scheme, sensor nodes utilize their geographic information to defeat the Denial of Service (DoS) attacks which are identified in [13]. Generally, actor nodes have more resources than sensor nodes in terms of communication, computation, battery, storage, *etc.* We further consider this asymmetric resources of actor and sensor nodes to design the proposed scheme.

The rest of this paper is organized as follows. In Section 2, we introduce preliminaries for our proposed scheme. In Section 3, we present our proposed scheme. In Section 4, we analyze the security and the performance of the proposed scheme. Finally, we conclude this paper in the Section 5.

2 Preliminaries

2.1 Security Requirements

In the subsection, we present the security requirements for AKA schemes in WSN. The AKA schemes should guarantee these requirements. Note that we only consider AKA between sensor and actor nodes. For AKA between actor nodes, existing AKA schemes [19, 20] are useful, so we do not address it. AKA between sensor nodes is an important research topic, but we remain it as our future work.

1. **Authentication:** The scheme should provide mutual authentication of two entities. That is, an attacker cannot impersonate a valid sensor or actor node without compromising the node. Even if a node is compromised, the scheme should guarantee that the attacker cannot impersonate other nodes except the compromised node.
2. **Key security:** After some two entities agreed a key, the scheme should guarantee that every entity except themselves and BS cannot compute the agreed key. The compromised node should not expose agreed keys of other nodes.
3. **Resilient to DoS attacks:** Karlof *et al.* introduced several DoS attacks for WSN[13]. They identified sybil attack, hello flood attack, and wormhole attack. The scheme should be secured against these attacks.

2.2 Bilinear Map

Let \mathbb{G}_1 be a cyclic additive group of prime order q and \mathbb{G}_2 be a cyclic multiplicative group of same order q . We assume that the discrete logarithm problem (DLP) in both \mathbb{G}_1 and \mathbb{G}_2 is intractable. We call $e: \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ a bilinear map if it satisfies the following properties:

1. Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_q^*$.
2. Non-degeneracy: There exists $P \in \mathbb{G}_1$ such that $e(P, P) \neq 1$.
3. Computability: There exists an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in \mathbb{G}_1$.

The Weil [15] and Tate [16] pairings in elliptic curve are examples of such a bilinear map.

2.3 Hard Problems

We assume that the following hard problems are intractable similar to [2, 3]. That is, there is no polynomial time algorithm solving these problems with non-negligible probability.

- **Computational Diffie-Hellman (CDH) problem:** The CDH problem is to compute abP when given, P, aP and bP for some a, b in \mathbb{Z}_q^* .
- **Modified Inverse Computation Diffie-Hellman (mICDH) problem:** The mICDH problem is to compute $(a + b)^{-1}P$ when given b, P, aP and $(a + b)P$ for some $a, b \in \mathbb{Z}_q^*$.
- **Bilinear Diffie-Hellman (BDH) problem:** the BDH problem is to compute $e(P, P)^{abc}$ when given P, aP, bP and cP for some $a, b, c \in \mathbb{Z}_q^*$.
- **Modified Bilinear Inverse Diffie-Hellman (mBIDH) problem:** The mBIDH problem is to compute $e(P, P)^{\frac{1}{a+b}c}$ when given b, P, aP and cP for some $a, b, c \in \mathbb{Z}_q^*$.

3 Our Proposed Scheme

In the section, we propose DoS-resilient AKA scheme between actor and sensor nodes in WSN. We consider asymmetric resource of sensor and actor nodes. Generally, actor nodes have more resources than sensor nodes, so, we try to assign less overheads for sensor nodes in the proposed scheme.

3.1 Assumptions

For the proposed scheme, we assume that actor nodes are resource-rich in terms of computation, storage and battery and have mobility. We further assume that the actor nodes have Global Positioning System (GPS) capability. These assumptions are general in WSN, and most security schemes for WSN [11, 12]

also assumed them. We assume that sensor nodes are low-power, low-cost devices such as MICA2 mote. The sensor nodes have no mobility, so they are static after deployment.

For deployment of sensor nodes, we assume that a practical approach such as [17, 18] is used. In the approach, mobile robots, which are similar to actor nodes, are used to deploy and localize individual sensor nodes. Before deployment, actor nodes (mobile robots) are equipped with several sensor nodes. Then, during deployment phase, the actor nodes drop the sensor nodes according to the predetermined plan. At that time, the actor nodes transmit the x and y coordinate values of the deployment position. During the deployment phase, we also assume that there is no compromise of the actor nodes.

3.2 Pre-deployment

Before deployment of sensor nodes, a trusted authority (TA) (*e.g.*, the system administrator or network planner) performs the following operations.

1. TA determines two groups $\mathbb{G}_1, \mathbb{G}_2$ and a bilinear map e as described in preliminaries.
2. TA chooses three cryptographic hash functions $h : \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$, $h_1 : \{0, 1\}^* \rightarrow \{0, 1\}^t$ and $h_2 : \mathbb{Z}_q^* \rightarrow \{0, 1\}^t$ where t is the size of session key.
3. TA computes $g = e(P, P)$, where P is a generator of \mathbb{G}_1 .
4. TA picks a secret value $\kappa \in \mathbb{Z}_q^*$ and then sets the public key of TA as $P_{pub} = \kappa P$.
5. For each actor node A_i , TA computes a public key as $PK_{A_i} = h(ID_{A_i})P + P_{pub}$ and a private key as $SK_{A_i} = (h(ID_{A_i}) + \kappa)$ where ID_{A_i} is identification information.
6. For each sensor node S_i , TA computes Id-Based Key as $IBK_{S_i} = h_2(\kappa h(ID_{S_i}))$.

TA then loads the public system parameters $(p, q, \mathbb{G}_1, \mathbb{G}_2, e, h, h_1, h_2, P, P_{pub}, g)$, ID_{A_i} , key pair (PK_{A_i}, SK_{A_i}) and κ into each actor node A_i . TA also loads the public system parameters $(p, q, \mathbb{G}_1, \mathbb{G}_2, e, h, h_1, P, P_{pub}, g)$, ID_{S_i} and IBK_{S_i} into each sensor node S_i .

3.3 Generation of Location-based keys

For deployment of sensor nodes, we assume the approach proposed in [17, 18]. This approach uses mobile robots (actor nodes) to deploy and localize sensor nodes. After pre-deployment is performed, each actor node equips several sensor nodes to deploy and receives deployment information from TA. The actor node then deploys sensor nodes according to the deployment information.

The proposed scheme utilizes the geographic information of a sensor node to generate its public key and private key pair. Therefore, actor node transmits a proper key pair to a sensor node when the sensor node is just deployed. They execute the following protocol.

$$\begin{aligned}
A_i &\longrightarrow S_i : \text{hello} \\
S_i &\longrightarrow A_i : ID_{S_i} \\
A_i &\longrightarrow S_i : Enc_{IBK_{S_i}}(ID_{S_i} || pos_{S_i} || LPK_{S_i} || LSK_{S_i})
\end{aligned}$$

An actor node first transmits a hello message to a sensor node S_i which is just deployed. After receiving this message, S_i replies its id ID_{S_i} . A_i then makes IBK_{S_i} and pos_{S_i} respectively as $IBK_{S_i} = h_2(\kappa h(ID_{S_i}))$ and $pos_{S_i} = (x_{S_i} || y_{S_i})$ where x_{S_i} and y_{S_i} are x and y coordinate values of the deployment position of S_i . A_i further generates location-based public and private key pair of S_i as $LPK_{S_i} = h(pos_{S_i})P + P_{pub}$ and $LSK_{S_i} = (h(ID_{S_i}) + \kappa)^{-1}P$. Finally, A_i encrypts ID_{S_i} , pos_{S_i} , PK_{S_i} and SK_{S_i} with a symmetric encryption scheme (e.g., AES and DES) and the symmetric key IBK_{A_i} and transmits the encrypted message to S_i . After receiving the message, S_i decrypts this message using the preloaded IBK_{S_i} , checks that it is valid and then stores pos_{S_i} , PK_{S_i} and SK_{S_i} . Note that when A_i finishes deployment process for all sensor nodes which A_i equips, A_i removes the secret value κ .

3.4 DoS-Resilient Authenticated Key Agreement

To authenticate and establish session keys, an actor node A_i and a sensor node S_i perform the following protocol.

$$\begin{aligned}
A_i &\longrightarrow S_i : ID_{A_i}, R_{A_i} \\
S_i &\longrightarrow A_i : pos_{S_i}, X, Y \\
A_i &\longrightarrow S_i : Z
\end{aligned}$$

A_i first generates a random value R_{A_i} from \mathbb{Z}_q^* and then transmits a message which consists of its id ID_{A_i} and R_{A_i} . After receiving it, S_i generates a random value R_{S_i} from \mathbb{Z}_q^* and computes sk , X and Y as $sk = h(g^r || R_{A_i} || pos_{S_i} || ID_{A_i})$, $X = R_{S_i}PK_{A_i} = R_{S_i}h(ID_{A_i})P + R_{S_i}P_{pub}$ and $Y = (R_{S_i} + sk)LSK_{S_i}$. S_i then sends pos_{S_i} , X and Y to A_i . When A_i receives this message, A_i first computes $e_{S_i} = e(X, SK_{A_i})$ and $sk' = h(e_{S_i} || R_{A_i} || pos_{S_i} || ID_{A_i})$. After computing e_{S_i} and sk' , A_i verifies that the following equation holds :

$$e(Y, h(pos_{S_i})P + P_{pub}) = e_{S_i}g^{sk'}$$

The verification works as follows

$$\begin{aligned}
e_{S_i} &= e(X, PK_{A_i}) = e(R_{A_i}h(ID_{A_i})P + R_{A_i}P_{pub}, (h(ID_{A_i}) + \kappa)^{-1}P) \\
&= e(R_{A_i}(h(ID_{A_i})P + \kappa P), (h(ID_{A_i}) + \kappa)^{-1}P) \\
&= e(R_{A_i}(h(ID_{A_i}) + \kappa)P, (h(ID_{A_i}) + \kappa)^{-1}P) \\
&= e(R_{A_i}P, P)^{h(ID_{A_i} + \kappa)h(ID_{A_i} + \kappa)^{-1}} \\
&= e(R_{A_i}P, P) = e(P, P)^{R_{A_i}} = g^{R_{A_i}}
\end{aligned}$$

and

$$e(Y, h(pos_{S_i})P + P_{pub}) = e((R_{S_i} + sk)LSK_{S_i}, (h(pos_{S_i}) + \kappa)P)$$

$$\begin{aligned}
&= e((R_{S_i} + sk)(h(pos_{S_i}) + \kappa)^{-1}P, (h(pos_{S_i}) + \kappa)P) \\
&= e((R_{S_i} + sk)P, P)^{(h(pos_{S_i}) + \kappa)^{-1}(h(pos_{S_i}) + \kappa)} \\
&= e((R_{S_i} + sk)P, P) = e(P, P)^{R_{S_i} + sk} \\
&= g^{R_{S_i} + sk} = g^{R_{S_i}} g^{sk} = e_{S_i} g^{sk} = e_{S_i} g^{sk'}
\end{aligned}$$

After this verification, A_i also verifies that S_i is really within the transmission range of S_i . That is, A_i checks that S_i is real neighbor node. A_i first finds its position values x_{A_i} and y_{A_i} from pos_{S_i} and then checks the following equation is valid.

$$(x_{A_i} - x_{S_i})^2 + (y_{A_i} - y_{S_i})^2 \leq R^2 \text{ where } R \text{ is transmission range of } S_i$$

If the all processes of verification are successful, A_i believes that S_i is valid and then computes two session keys, Mackey and Enckey as $Mackey = h_1(sk || pos_{S_i} || ID_{A_i} || 0)$ and $Enckey = h_1(sk || pos_{S_i} || ID_{A_i} || 1)$. A_i also computes a message authentication code Z as $MAC_{Mackey}(pos_{S_i} || ID_{A_i})$ where MAC is a message authentication code function and then sends Z to S_i . After receiving Z , S_i first computes Enckey and Mackey and then checks Z is valid. If Z is valid, the overall process of the scheme succeeds, and A_i and S_i share two keys, Mackey and Enckey. Otherwise, it fails.

4 Analysis

4.1 Security Analysis

Security of IBK: The proposed scheme utilizes IBK to distribute the LBK.

For a sensor node S_i , because we assume that the DLP is intractable in \mathbb{G}_1 , an adversary cannot obtain $LBK_{S_i} = h_2(\kappa h(ID_{S_i}))$ without the secret value κ . After the deployment of sensor nodes, all nodes including actor and sensor nodes do not have κ , so the adversary cannot obtain LBK_{S_i} .

Authentication: The proposed scheme provides mutual authentication between an actor node A_i and a sensor node S_i . A_i checks whether $e(Y, h(pos_{S_i})P + P_{pub}) = e_{S_i} g^{sk'}$ holds. If it holds, A_i can verify that S_i has the knowledge of sk' and LSK_{S_i} and then believes that S_i is valid. S_i also can verify that A_i has the knowledge of sk and SK_{A_i} by checking $Z = MAC_{Mackey}(pos_{S_i} || ID_{A_i})$. If it holds, S_i believes that A_i is valid.

Security of session key: In the proposed scheme, the security of session keys is based on the intractability of the mBIDH problem. By eavesdropping, an adversary can obtain $h(ID_{A_i})$, P , $P_{pub} = \kappa P$ and $R_{S_i}(h(ID_{A_i}) + \kappa)P$. But, the attacker cannot compute $e_{S_i} = g^r = e(P, P)^{(\kappa + h(ID_{A_i}))^{-1} R_{S_i}(h(ID_{A_i}) + \kappa)}$ and $sk = sk'$ because she do not know the secret value κ and there is no polynomial time algorithm solving mBIDH problem with non-negligible probability [2].

Resilient to DoS attacks: In the following, we demonstrate how our proposed scheme can act as countermeasures against some most famous attacks which identified in [13, 14].

- **Sybil attack:** Sybil attack [13, 14] is performed by a malicious sensor node which behaves as if it were a large number of nodes. That is, a node impersonates other nodes or simply claiming multiple forged identities. Sybil attack is extremely harmful to many important tasks of WSAAN such as routing and data aggregation of actor nodes. In our proposed scheme, sensor nodes utilize their LBK which contains their location information. To perform sybil attack in our proposed scheme, an adversary should have to forge LBK of other nodes or compromise valid nodes. Because to forge LBK is depend on mBIDH problem, the adversary cannot impersonate other nodes. In addition, when the adversary compromise a valid node, she can utilize information of the compromised node in only the transmission range of the compromised node because our proposed scheme checks whether a sensor node exists in its transmission range.
- **Identity replication attack:** Identity replication attack [14] happens when an adversary loads multiple replicas of a compromised node in different geographic locations. This attack causes actor nodes get the faked data from replicated nodes. As mentioned above, because LBK contains geographical information of sensor nodes, actor nodes can confirm whether a sensor node really exist in the transmission range. If an adversary cannot forge LBK, we can reduce the effect of this attack. That is, the attack can be performed in the transmission range of the compromised node.
- **Wormhole attack:** In wormhole attacks, two malicious nodes, which are connected with low-latency communication link, are deployed in a little distant location. By collecting messages and relaying them, they make that their neighbor nodes are confused as if they coexist in closed range where they communicate each other. This attack can jeopardize routing and data aggregation. In our proposed scheme, LBK which contains the geographical information of sensor nodes is utilized, so an adversary can perform this attack only if she can forge LBK which depends on mBIDH problem.

4.2 Performance Analysis

In the performance, the proposed scheme satisfies our design goal in which sensor nodes have less overheads. In the proposed scheme, the sensor nodes do not perform pairing operation which is several times more costly than a scalar multiplication. Instead, the sensor nodes need several scalar multiplication computations for each AKA. Compared with other DoS-resilient scheme [9, 10] which each entity should compute one pairing operation, in our proposed scheme, only actor nodes perform pairing operation and sensor nodes need not compute it.

Furthermore, because the proposed scheme utilizes the ID-based cryptosystem, and the entities need not transmit their public-key certificates, the proposed scheme can obtain low communication overhead for both actor and sensor nodes compared with Yu *et al.*'s scheme [11]. Yu *et al.*'s scheme utilize the merkle hash tree to reduce the need of transmitting certificates of public key. Their approach is not scalable. When the number of nodes increases, the communication cost also increases.

In the proposed scheme, the actor nodes should compute one Weil or Tate pairing. Because the actor nodes have enough resources in terms of storage and battery, the only computation time of the pairing is an issue. In the recent implementation [4], the computation of pairing in a sensor node only takes 1.93 sec. This result shows the feasibility to utilize pairing operation in actor nodes.

5 Concluding Remarks

In this paper, we have proposed DoS-resilient authentication key agreement scheme in which sensor nodes utilize the geographic information as their identity information to defeat the DoS attacks identified in [13]. Furthermore, in the proposed scheme, sensor nodes have less overhead in terms of communication and computation since the sensor nodes do not perform pairing computation and transmit the public-key certificates.

The proposed scheme is an intermediate result to design full AKA scheme for WSAAN. In this paper, we only have addressed the AKA problem between actor and sensor nodes. In the future, we will propose the full AKA scheme by addressing sensor-sensor AKA and actor-actor AKA problems. In addition, only sensor nodes utilize the geographic information as their identity information in the proposed scheme. Therefore, when an actor node is compromised, the proposed scheme cannot defeat the DoS attack with the compromised actor node. We will also address this problem in the near future.

Acknowledgements

This work was supported by the National Security Research Institute (NSRI) of Korea under grant 2009_018.

References

1. I. F. Akyildiz and I. H. Kasimoglu, "Wireless sensor and actor networks: research challenges", Ad Hoc Networks, Vol. 2, Issue 4, pp. 351-367, 2004.
2. K. Choi, J. Hwang, D. Lee and I. Seo, "ID-based authenticated key agreement for low-power mobile devices", ACISP 2005, LNCS 3574, pp. 494-505, 2005.
3. Y. Kim, H. Lee, J. Park and L. T. Yang, "Key establishment scheme for sensor networks with low communication cost", ATC 2007, LNCS 4610, pp. 441-448, 2007.

4. M. Shirase, Y. Miyazaki, T. Takagi, D. Han and D. Choi, "Efficient implementation of pairing based cryptography on a sensor node", IEICE Trans. on Information and Systems, vol. E92-D, No. 5, pp. 909-917, 2009.
5. R. Vedanthan, Z. Zhuang and R. Sivakumar, "Mutual exclusion in wireless sensor and actor networks", IEEE SECON 2006, pp. 346-355, 2006.
6. J. Wu, S. Yang and M. Cardei, "On maintaining sensor-actor connectivity in wireless sensor and actor networks", IEEE INFCOM 2008, pp. 888-896, 2008.
7. L. Eschenauer and V. D. Gligor, "A key management scheme for distributed sensor networks", ACM CCS'02, pp. 41-47, 2002.
8. H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks", IEEE Symposium on Security and Privacy, pp. 197-213, 2003.
9. Y. Zhang, W. Liu, W. Lou and Y. Fang, "Securing sensor networks with location-based keys", IEEE WCNC 2005, pp. 1909-1914, 2005.
10. Y. Zhang, W. Liu, W. Lou and Y. Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks", IEEE JSAC, Vol. 24, No. 2, pp. 1-14, 2006.
11. B. Yu, J. Ma, Z. Wang, D. Mao and C. Gao, "Key establishment between heterogeneous nodes in wireless sensor and actor networks", APWeb Workshops 2006, LNCS 3842, pp. 196-205, 2006.
12. X. Cao, M. Huang, Y. Chen and G. Chen, "Hybrid authentication and key management scheme for WSANs", ISPA Workshops 2005, LNCS 3759, pp. 454-465, 2005.
13. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", Ad Hoc Networks, Vol. 1, Issues 2-3, pp. 293-315, 2003.
14. J. Newsome, E. Shi, D. Song and A. Perrig, "The sybil attack in sensor networks: Analysis & defenses", IPSN 2004, April 2004.
15. D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing", SIAM Journal of Computing, Vol. 32, No. 3, pp. 586-615, 2003.
16. P. Barreto, H. Kim, B. Bynn and M. Scott, "Efficient algorithms for pairing-based cryptosystems" CRYPTO '02, LNCS 2442, pp. 354-368, 2002.
17. P. Corke, R. Peterson and D. rus, "Networked robots: flying robot navigation using a sensor net" ISRR '03, 2003.
18. A. Sanfeliu and J. Andrade-Cetto, "Ubiquitous networking robotics in urban settings", Workshop on Network Robot Systems, 2006.
19. Muhammad Bohio and Ali Miri, "Efficient identity-based security schemes for ad hoc networks routing protocols", Ad Hoc Networks Vol. 2, pp. 309-317, 2004.
20. Hung-Yu Chien and Ru-Yu Lin, "Improved id-based security framework for ad hoc network", Ad Hoc Networks vol. 6, pp. 46-60, 2008.