Efficient Sensor Node Authentication via 3GPP Mobile Communication Networks

Kyusuk Han
KAIST
119 Munjiro, Yuseonggu, Daejeon
hankyusuk@kaist.ac.kr

Jangseong Kim
KAIST
119 Munjiro, Yuseonggu, Daejeon
jskim.withkals@kaist.ac.kr

Kwangjo Kim
KAIST
119 Munjiro, Yuseonggu, Daejeon
kkj@kaist.ac.kr

Taeshik Shon
Samsung Electronics, Inc.
Suwon, Korea
ts.shon@samsung.com

ABSTRACT

Energy efficiency is one of important issues in the resource constrained wireless sensor network. In this paper, we propose the authentication and key agreement protocol that efficiently reduces the overall computational and communication costs in the next generation converged network. The enhanced security procedures are operated through the mobile network in order to maximize the lifetime of the sensor networks and to apply the combined capabilities of both networks.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and protection*; C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Network communications, Wireless communication*

General Terms

Security

Keywords

Mobile Netwok, Wireless Sensor Network, Authentication, Key Agreement, 3G-WSN

1. INTRODUCTION

As a *de facto* standard for the wireless sensor networks (WSNs), Zigbee [3] specifies the security functions that the key agreement architecture is operated by using keys that are pre-distributed. However, it is hard to assume the pre-distribution of keys in large scale network. Thus, many active researches such as [1, 2, 8] are continued in order to provide efficient authentication and key distribution in WSNs.

Ibriq and Mahgoub [5] proposed an efficient hierarchical key establishment model with 'partial key escrow table'. Using the key escrow table, a sink can self-generate the shared key for the attached nodes: An intermediate sink has a partial key escrow table that stores the partial information of nodes. After the requests from nodes are received, the sink request the authentication ticket to the base station. After receiving the ticket, the sink authenticates and shares keys with nodes.

CCS'10, October 4–8, 2010, Chicago, Illinois, USA.
ACM 978-1-4503-0244-9/10/10.

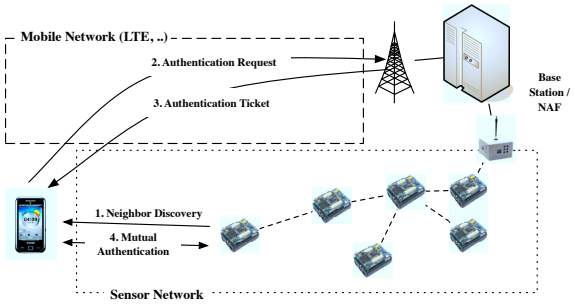

Figure 1: Proposed system model integrates a sensor network as one of application into the mobile communication network.

Therefore, our motivation is to bring the more benefits from the consolidation of WSNs and 3G mobile network (3G-WSN) based on the standard architecture. We propose an efficient and secure authentication and key exchange protocol between sensor nodes and the smartphone with sensors. Since the efficient resource management is one of the most important requirements in WSNs, our approach concentrates on how to minimize the energy consumption and inefficient message transmission.

2. AUTHENTICATION VIA MOBILE NETWORK

2.1 System model

Figure 1 shows our proposed model that the sensor attached smart phone communicates to the authentication server via mobile network, and directly communicates to the sensor. In the architecture, the sensor network can be a kind of third party application in the mobile network applying the generic authentication architecture (GAA) [7].

The sensor attached smartphone as a mobile device (MD) has GAA module and Zigbee module. The network consists of mobile network entities such as a bootstrapping server

function (BSF) and a network application function (NAF), and the sensor network entity such as sinks. For more detail of BSF and NAF, please refer [7]. We assume that a sensor network consists of a base station and sensor nodes (sinks). When sinks are deployed, each sink shares a unique key with the base station. The establishment of the sensor network can follow any previous security protocols such as [5, 8] and is out of scope in this paper.

Table 1: Notations

Type	Description
S_i	Sensor node, a sink i
$MAC_k(m)$	MAC of a message m using key k
$e_k\{m\}$	Encrypt m using k
$h(m)$	Hash output of m
TS	Timestamp
CK_i	Cipher key of an entity i
IK_i	Integrity key of an entity i
KDF	Key derivation function

2.2 Protocol Description

The protocol is mainly divided into two parts: Phase 1 is operated in the mobile network, and Phase 2 is operated in the sensor network. We show the notations and the message types used in the protocol in Table 1. M_REQ and M_RES are transmitted in Phase 1 via mobile network. S_REQ, S_RES, S_CON are the messages transmitted in Phase 2 via the sensor network.

2.2.1 Pre-Phase: Neighbor Discovery

Every sensor periodically broadcasts HELLO message to find the neighbor sensors. A sink S_1 periodically broadcasts $HELLO$ with u_0 and v_0, where $u_0 = e_{CK_{S_1}}\ \{R_0||TS\}$ and $v_0 = MAC_{IK_{S_1}}\ (u_0)$. R_0 is a random nonce selected by S_1, and TS is a timestamp.

When MD receives the $HELLO$ message from S_1 already authenticated, MD ignores this phase. Thus, the energy cost and message size of this phase is not considered for the performance analysis of this protocol.

2.2.2 Phase 1: Authentication via Mobile Network

When MD is firstly joining the network, MD has to share keys CK_{MD} and IK_{MD} with the serving network using GAA. When unauthenticated MD receives $HELLO$ from S_1, MD requests the authentication of S_1 to the NAF. MD generates u_1 using CK_{MD} and v_1 using IK_{MD}, where $u_1 = e_{CK_{MD}}\{S_1||u_0||v_0\}$ and $v_1 = MAC_{IK_{MD}}(MD||u_1)$. After that MD send u_1 and v_1 to NAF.

$$MD \rightarrow NAF : M\_REQ||MD||u_1||v_1$$

If NAF has no information of MD, NAF asks BSF about MD and obtains CK_{MD} and IK_{MD} from GAA process. NAF then generates u_2 and v_2, where $u_2 = e_{CK_{S_1}}\{h(R_0$ $||CK_{MD})||\ h(R_0||IK_{MD})\}$ and $v_2 = MAC_{IK_{S_1}}\ (R_0||u_2)$. NAF also generates u_3 and v_3, where $u_3 = e_{CK_{MD}}\{R_0||$ $TS||h(R_0||CK_{S_1})||h(R_0||IK_{S_1})||\ u_2||v_2\}$ and $v_3 = MAC_{IK_{MD}}$ $(M\_RES||u_3)$. And, the NAF sends u_3 and v_3 to MD.

$$NAF \rightarrow MD : M\_RES||MD||u_3||v_3$$

After verifying v_3 and decrypting u_3, MD retrieves R_0, $h(R_0||CK_{S_1})$ and $h(R_0||IK_{S_1})$. Then MD generates CK_{S_1MD} and IK_{S_1MD}, shared session keys between MD and S_1, using one way function KDF, as follows:

$$CK_{S_1MD} = KDF(h(R_0||CK_{S_1})||h(R_0||CK_{MD}))$$

$$IK_{S_1MD} = KDF(h(R_0||IK_{S_1})||h(R_0||IK_{MD}))$$

2.2.3 Phase 2: Mutual Authentication between MD and Sensor

After the authentication process between MD and NAF, MD generates the shard session keys CK_{S_1MD} and IK_{S_1MD}. MD computes v_4 using IK_{S_1MD}, where $v_4 = MAC_{IK_{S_1MD}}$ $(S\_REQ||MD||S_1||R_0||u_2||v_2)$ and sends v_4 with u_2 and v_2 to S_1 as follows.

$$MD \rightarrow S_1 : S\_REQ||MD||S_1||u_2||v_2||v_4$$

When S_1 receives u_2, v_2 and v_4, S_1 checks the validity of v_2 at first. After that S_1 decrypts u_2 and retrieves $h(R_0||CK_{MD})$ and $h(R_0||IK_{MD})$. S_1 generates IK_{S_1MD} with $h(R_0||IK_{MD})$ and verifies v_4. Finally, S_1 generates v_5 as the response to MD, where $v_5 = MAC_{IK_{S_1MD}}(S\_RES$ $||S_1||MD||R_0)$ and sends it to MD as follows:

$$S_1 \rightarrow MD : S\_RES||S1||MD||v_5$$

After MD verifies v_5, MD generates v_6 for the confirmation of the authentication response, where $v_6 = MAC_{IK_{S_1MD}}$ $(S\_CON||MD||S_1||R_0 + 1)$ and sends it to S_1 as follows:

$$MD \rightarrow S_1 : S\_CON||MD||S_1||v_6$$

$R_0 + 1$ is the update of R_0 with addition and used for the freshness check, and can be substituted with other methods. S_1 completes the authentication of MD by checking the validity of v_6.

3. ANALYSIS

In this section, we show the analysis of the proposed protocol. At first, we show the security analysis of our proposed protocol, and then show the efficiency of our proposed design by comparing with the previous models.

3.1 Security of Proposed Protocol

We analyze the security of our protocol against key compromise, message forgery and several known attacks.

3.1.1 Security Against Key Compromise

The share session keys are initially generated using the master seed key stored in USIM. Since the transmitted key generating informations are encrypted, an adversary $\mathcal{A}$ fails to know such information. Also, the shared session keys CK and IK are generated using R_0.

Assume the node S_1 is compromised, $\mathcal{A}$ may try to know the value of CK_{MD} and IK_{MD} in order to impersonate MD. However, $\mathcal{A}$ is only able to generate the shared session key between MD and S_1 using the only known informations of MD are $h(R_0||CK_{MD})$ and $h(R_0||IK_{MD})$. $\mathcal{A}$ cannot know CK_{MD} from $h(R_0||CK_{MD}$ due to the *one-wayness* of cryptographic hash function.

3.1.2 Security Against Message Forgery

In our protocol, every packet is protected by Message Authentication Code (MAC). An adversary $\mathcal{A}$ should be able to forge MAC to success the attack. Thus, our protocol is secure against the man-in-the-middle attack while the adversary has no efficient way to forge MAC.

3.1.3 Security against known attacks

Since the most parts of the proposed protocol are operated in the mobile networks, most attacks on the sensor network [6] do not affect on the proposed protocol. Thus we only consider the security of Phase 2 that the direct authentication process between MD and S_1.

The replay attack fails in the protocol due to the random nonce used in the packet at each session. Wormhole attack on our protocol fails since the adversary cannot send the confirmation message. Spoofed, altered or replayed routing information attacks also fail without knowing encrypted nonce in our protocol. The sinkhole attack against our protocol fails without knowing the keys. Sybil attacks also fails from verification of identity of nodes.

3.2 Performance Comparison

We compare our proposed model with Ibriq and Mahgoub's protocol [5] that provides significant efficiency for WSNs. For measuring the approximate communication overheads in each design, we defined the message size with MAC size as 4 bytes, the time stamp as 8 bytes, nonce as 8 bytes, and key size as 16 bytes as shown in [1]. And, We set the source and target IDs as 1 byte, respectively. For our protocol, we also set the message types as 1 byte. We refer the energy cost for the transmitting the messages are estimated based on the experimental results in [4], which used the MICAz running at 7.37 MHz and TelosB at 4 MHz for application data rates of respectively 108 kbps and 75 kbps. Based on the such results, our proposed protocol shows approximately 172 μJ in the authentication between MD and a sink, concentrating the most communication to the mobile network.

Table 2: Comparison

Protocol	Ibriq [5]	Proposed
System Model	WSN	3G -WSN
Interworking	N/A	GAA [7]
Nodes for Authentication	5	1
Energy (μJ)	707	172
Tot. Msg. (bytes)	744	33
Tot. Eng. (μJ)	3,869	172

Table 2 shows the more detailed comparison for authenticating MD. Our protocol shows the significant efficiency compared with previous model. Since only two nodes are involved in the communication under the sensor network in Phase 2, overall message size is small and static. Energy cost for transmission is also dropped by about 90 percent than the previous protocol. The computation overhead is not considered for the performance analysis, since such overhead is negligibly lower than in the communication. Although there is additional energy cost in Phase 1, we can ignore such overhead because a mobile phone can be daily recharged in general.

Therefore, the separated communication suited application's purpose in 3G network and WSN enables us to use the maximized benefits of the consolidated network, the more applicable architecture.

4. CONCLUSION

Secure and efficient interworking of several different networks is the important issue in the next generation convergence network. In this paper, we proposed an efficient authentication and key exchange protocol for the 3G-WSN network by integrating WSN into 3G network as the application. While most communications are operated under the mobile network, the communication in the sensor network is minimized than previous work. When the hop distance between end-to-end nodes are five in the sensor network, energy cost in the sensor network applying our proposed design is estimated to be dropped by about 90 percent than previous models.

5. REFERENCES

[1] J. Abraham and K. S. Ramanatha. An efficient protocol for authentication and initial shared key establishment in clustered wireless sensor networks. *Proceeding of Third IFIP/IEEE International Conference on Wireless and Optical Communications Networks*, 2006.

[2] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. *in IEEE Symposium on Security and Privacy, Berkeley, California*, pages 197–213, May 11-14 2003.

[3] W. C. Craig. Zigbee:Wireless control that simply works. *Zigbee Alliance*, 2005.

[4] G. de Meulenaer, F. Gosset, F. X. Standaert, and L. Vandendorpe. On the Energy Cost of Communications and Cryptography in Wireless Sensor Networks. In *(extended version), IEEE International Workshop on Security and Privacy in Wireless and Mobile Computing, Networking and Communications (SecPriWiMob'2008)*, pages 580–585, 10 2008.

[5] J. Ibriq and I. Mahgoub. A hierarchical key establishment scheme for wireless sensor networks. *Proceedings of 21st International Conference on Advanced Networking and Applications (AINA'07)*, pages 210–219, 2007.

[6] C. Karlof and D. Wagner. Secure routing in wireless sensor networks. *In Proc. of SNPA'03, Anchorage, Alaska*, pages 113–127, May 2003.

[7] Third Generation Partnership (3GPP). *TS 33.220 v9.2.0 Generic Authentication Architecture(GAA); Generic Bootstrapping Architecture (Release 9)*, Dec. 18 2009.

[8] S. Zhu, S. Setia, and S. Jajodia. LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. *ACM Trans. Sen. Netw.*, 2(4):500–528, 2006.