ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Efficient Sensor Node Authentication via 3GPP Mobile Communication DOC

D. Prasad
Research Scholar,
Annamalai University, Chidambaram,
Associate Professor,
Ramanandatirtha Engineering College, Nalgonda .

E. Satheesh Kumar
Associate Professor,
Ramanandatirtha Engineering College,
Nalgonda.

ABSTRACT:

Energy efficiency is one of important issues in the re- source contrained wireless sensor network. In this paper, we pro- pose the authentication and key agree- ment protocol that efficiently reduces the overall computational and communi- cation costs in the next generation converged network. The enhanced secu- rity procedures are operated through the mo- bile net- work in order to maximize the lifetime of the sensor networks and to apply the combined capabilities of both networks.

Keywords:

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

INTRODUCTION:

As a de facto standard for the wireless sensor net- works (WSNs), Zigbee species 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 are con- tinued in order to provide e_cient authentication and key distribution in WSNs. Ibriq and Mahgoub 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. 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 be- tween sensor nodes and the smartphone with sensors. Since the e_cient resource management is one of the most important requirements in WSNs, our approach concentrates on how to minimize the energy con- sumption andin efficient message transmission.There- fore, 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 pro- pose an efficient and secure authentication and key ex- change protocol between sensor nodes and the smart phone with sensors. Since the efficient resource man- agement is one of the most important requirements in WSNs, our approach concentrates on how to minimize the energy consumption and inefficient message trans- mission.

2. AUTHENTICATION VIA MOBILE NETWORK:

2.1 System model:

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 net- work applying the generic authentication architecture (GAA).

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The sensor attached smart phone 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 .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 and is out of scope in this paper.

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 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 end the neighbor sensors. A sink S1 periodically broadcasts HELLO with u0 and v0, where u0 = eCKS1 fR0jjTSg and v0 = MACIKS1(u0).R0 is a random nonce selected by S1, and TS is a timestamp. When MD receives the HELLO message from S1 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 _rstly joining the network, MD has to share keys CKMD and IKMD with the serving network using GAA. When unauthenticated MD receives HELLO from S1, MD requests the authentication of S1 to the NAF. MD generates u1 using CKMD and v1 using IKMD, Where u1 = eCKMDfS1jju0jjvog and v1 = MACIKMD(MDjju1). After that MD send u1 and v1 to NAF.MD ! NAF:M REQjjMDjju1jjv1 If NAF has no information of MD, NAF asks BSF about MD and obtains CKMD and IKMD from GAA process. NAF then generates u2 and v2, where u2 = eCKS1 fh(RojjCKMD)jj h(RojjIKMD)g and v2 = MACIKS1 (Rojju2).

NAF also generates u3 and v3, Where 3=eCKMDfRojj TSjjh(RojjCKS1)jjh(RojjIKS1)jj u2jjv2g and v3 = MACIKMD (M RESjju3).And, the NAF sends u3 and v3 to MD.NAF ! MD : M RESjjMDjju3jjv3After verifying v3 and decrypting u3, MD retrieves R0, h(RojjCKS1) and h(RojjIKS1). ThenMD generates CKS1MD and IKS1MD, shared session keys between MD and S1, using one way function KDF, as follows:CKS1MD = KDF(h(RojjCKS1) jjh(RojjCKMD)) IKS1MD = KDF(h(RojjIKS1) jjh (RojjIKMD))

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 CKS1MD and IKS1MD. MD computes v4 using IKS1MD, where v4 = MACIKS1MD (S REQjjMDjjS1jjRojju2jjv2) and sends v4 with u2 and v2 to S1 as follows. MD! S1 :S REQjjMDjjS1jju2jjv2jjv4

3. ANALYSIS:

In this section, we show the analysis of the proposed protocol. At _rst, we show the security analysis of our proposed protocol, and then show the e_ciency 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 com- promise, 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 A fails to know such information. Also, the shared session keys CKand IK are generated using R0. Assume the node S1 is compromised, A may try to know the value of CKMD and IKMD in order to impersonateMD. However, A is only able to generate the shared session key between MD and S1 using the only known informations of MD are h(RojjCKMD) and h(RojjIKMD). A cannot know CKMD from h(RojjCKMD due to the one-wayness of cryp- tographic hash function.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

3.1.2 Security Against Message Forgery:

In our protocol, every packet is protected by Message Authentication Code (MAC). An adversary 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 do not a_ect on the proposed protocol. Thus we only consider the security of Phase 2 that the direct authentication process between MD and S1. 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 that provides significant efficiency for WSNs. For measuring the approximate communication over-heads in each design, we de_ned 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 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 _J in the authentication between MD and a sink, concentrating the most communication to the mobile network.

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 ve in the sensor network, energy cost in the sensor network applying our proposed de- sign 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.