한국컴퓨터정보학회 하계학술대회 논문집 제20권 제2호 (2012. 7)

USN에서의 이동성을 위한 핸드오버 인증 프로토콜

니반제 브루스*, 김태용**, 이훈재°
*동서대학교 대학원 유비쿼터스IT학과
°**동서대학교 정보통신공학전공
e-mail:{ndibabruce@gmail.com}*, {tykimw2k, hjlee@dongseo.ac.kr}**°

Handover Protocol for Mobility Support in Ubiquitous Sensor Network

Ndibanje Bruce*, TaeYong Kim**, HoonJae Lee°
*Dongseo University, Dept. Ubiquitous IT
°**Dongseo University, Dept. Information & Comm. Eng.
e-mail:{ndibabruce@gmail.com}*, {tykimw2k, hjlee@dongseo.ac.kr}**°

● Abstract ●

The System of communication with wireless devices is experiencing a huge growth. While traditional communication paradigms deal with fixed networks, mobility raises a new set of questions, techniques, and solutions. In order to realize service mobility, there is a need of protocol that can support mobility while nodes are communicating without any disruption of their connection status. This paper proposes a handover authentication protocol for mobility support. Careful considerations must be taken in priority to security issues since many unreliable public and private resources; both networks and devices are involved. The protocol is based on public key cryptography with Diffie-Hellman algorithm which provides security against both leakage-resilience of private keys on untrustworthy devices and forward secrecy

키워드: 인증 프로토콜, 핸드오버 (Handover), 핸드 오프 (Handoff), 이동성

I. Introduction

Service mobility is spotlighted on the need to retain access to service across different devices and networks in ubiquitous computing environment. Wireless sensor network (WSN) applications such as patients' health monitoring in hospitals, location-aware ambient intelligence, and industrial monitoring /maintenance or homeland security require the support of mobile nodes or node groups. In many of these applications, the lack of network connectivity is not admissible or should at least be time bounded, i.e. mobile nodes cannot be disconnected from the rest of the WSN for an undefined period of time In this context, we aim at reliable and real-time mobility support in WSNs, for which appropriate handoff and rerouting decisions are mandatory. This concerns both individual nodes and node groups (e.g. body sensor network) mobility – usually dubbed as "physical mobility". Public wireless local area network (WLAN) systems based on IEEE 802.11 are exponentially becoming popular in hot spot areas such as airports, campuses, convention centers, and so on. Unlike existing wireless Internet services based on cellular networks, public WLAN systems can provide high-speed Internet connectivity up to 11Mbps (IEEE 802.11b [1]) or 54Mbps (IEEE 802.11a/g [2], [3]).

However, the advances of public Wi-Fi services and multimedia applications have raised an unforeseen problem, handoff support between access points (APs) [4]. Due to insufficient handoff support in IEEE 802.1 networks, a significant disruption can be experienced while a handoff is performed. Furthermore, the current WSN protocols do not permit to fulfill reliability and real-time requirements under physical mobility. Mobility support in WSNs is in its preliminary steps, since the majority of the current WSN applications assume nodes are static. The Bluetooth [5] LMP

performs link supervision to detect events such as if the device at the other end has moved out of range. If this has happen, a link supervision timer will elapse and allow the link to be shut down, so that its active member address can be reused. The logical solution for the remote end device is to involve itself in a handover mechanism if it is willing to still form part of the network. However handover is not supported by Bluetooth as J. Bray and C. F. Sturman describe in [5] and therefore the effective range of a network is constrained to the range of a piconet. The handover procedure also needs to protect its message integrity, confidentiality, and replay attack to prevent from hijacking connectivity and disrupting service. Many researches on service mobility are carried over. Most of these researches consist of servers which manage service migration, i.e. SIP and Universal Inbox. However, nomadic mobile user and diverse services make difficult to manage the service mobility.

In this paper, we proposed a handover authentication protocol where a mobile device initiates a commutation to a given access point and while commutating, the use moves to another access point which handles the communication between the users. This protocol supports the mobility while the initiator moves within the access points.

II. Related Works

Mobility in Wireless Sensor Networks is a topic greatly mentioned in the WSN literature, where different solutions have been defined in function whether the domain is changed or not, inter-mobility and intramobility respectively, other type of mobility can be considered in function what is moving i.e. node or network, and whether it is assisted by a proxy. Several authentication protocols have been proposed for wired networks such as Kerberos and SSL. Kerberos uses symmetric key methods, which are ideal for network environments where all services and clients are known in advance.

This is habitually not the case in a WMN where clients may join, leave and move freely at will. To perform authentication, the SSL uses public key methods (e.g., public key certificates), which is ideal for secure communications with a large, variable user base that is not known in advance, such as the Internet. However, public key methods are computationally intensive and space consuming, which are not suitable for resource-constrained mobile devices.

The current IEEE 802.11i and 802.11s standards do not support fast re-authentication or fast hand-off in general, when a client moves from one MAP (or network) to another. In mobile IP and cellular networks, the foreign agent/network must communicate with a client's home agent/network via multi-hop communications to authenticate the client. The most common models are the standard techniques, which are used in cellular, wireless mesh, WLAN, and 6LoWPAN networks.

The use of this technique in wireless sensor networks is not recommended, since nodes are usually deployed in a harsh environments and low cost radio transceivers and antennas are usually used, at least for large scale WSN scenarios, hence the received signal strength is not stable. Therefore, relying on only one (unreliable) metric may lead to a poor handoff decision.

III. Handover Authentication Protocol

This section describe the proposed handover authentication protocol based Public Key Cryptography with Diffie Hellman algorithm. We consider a Healthcare Hospital with Ubiquitous Sensor Network, where a nurse or Doctor can access data from his wireless mobile device. The procedure of the initial authentication is triggered when the nurse/doctor want to access the patient's data via a given access point. Then, while they are moving inside of the hospital, they keep communicate with the wireless healthcare system trough different access point. To keep this communication among the access points, the handover authentication protocol is invoked to support the mobility management.

We assume that the registration phase is already done by the management of the wireless healthcare system and each stuff member has to keep in secrecy his authentication parameters such as ID and pass word for subsequent utilizations.

1. Initial User Authentication

This phase is performed when there is a start of new session.

The user (nurse or doctor) initiates a request to the nearby access point and the procedure of the initial authentication begins as follows:

First the user U sends a request message for authentication (RqMAuth) to the current access point.

$$U \rightarrow APcurr : RqMAuth,$$
$$RqMAuth = (Iu, PW)_{Ku}, CurrT.$$

The user id and the password are encrypted with Deffie Hellman value (Ku) by hashing the defined parameters to

render more secure the value. The value is computed as follows:

$$Ku = g^{h(RIu||IAPcurr||CurrT)} \bmod p.$$

After receiving the RqMAuth from the user, the current access point performs the following:

1) The current access point generates a random number Rw and computes its private key in order the decrypt the request message for authentication $SK_{APcurr} = g^{h(Rw||IAPcurr)} \bmod p.$

Table 1. Notations and descriptions

Notations	Descriptions
U	Nurse or Doctor User
Pw	User Password
Iu	User ID
RIu	Random number of user
APcurr	Current Access Point
APnew	New Access Point
IAPcurr	ID of Current AP
IAPnew	ID of New AP
CurrT	Current Time
NewT	New Time
H (.)	Cryptographic hash function e.g SHA1 SHA2

Table 1 gives some of the notations and of the parameters we use in this paper.

2) The A Pcurr decrypt the RqMAuth obtain RIu , Iu and PW from message decryption, then check if the user id and password much with the ones stored if yes performs the next step otherwise reject the request, then randomly chooses Rw and the session_id(Sess_id) to identify to ongoing service session between user U and Ipcurr, it stay the same until the end of the session.

3) The APcurr send back to U the response message authentication (ResMAuth) encrypted with KAPcurr which is Diffie-Hellman value computed by the current access point, then sends to the user the following:

$$APcurr \rightarrow U: ResMAuth,$$
$$ResMAuth = (IAPcurr, Rw, Sess-id, RIu)_{K_{APcurr}}$$

where the $KAPcurr = g^{h(Rw||CurrT)} \bmod p.$

Upon receiving the ResMAuth, the user performs the decryption with $SKIu = g^{h(RIu||Iu)} \bmod p$ and verify if RIu matches with the one sent to the access point, if yes continues the operation otherwise abort.

The use sends an authentication acknowledge message (AckMAuth) to the access point:

$$U \rightarrow APcurr: AckMAuth,$$
$$AckMAuth = (RW)_{Ku},$$

Once upon the APcurr receives the AckMAuth, it performs the decryption and checks if the received value matches with the one sent if yes continues to the next step otherwise abort the operation. Finally the entities compute a session key for subsequent message after this tree-way handshake.

$$SessK = H(RIu||Rw).$$

This is the end of initial user authentication phase.

2. Handover User Authentication Protocol

The handover protocol is invoked when the user want to switch to the new access point from the old one. This protocol handles the mobility of the user and supports the continuity of the session.

In this phase, the user migrates the session service from current access point to the new access point.

The user with his mobile device sends the handover authentication request (ReqHAuth) to the new access point as following:

$$U \rightarrow APnew: RqHAuth$$
$$RqHAuth = (NewT, Iu, (Sess-id)_{SeeK})_{Ku}, NewT$$

where RIu* is the new random number with the encryption of $Ku = g^{h(RIu^*||IAPnew||NewT)} \bmod p.$

When the APnew receives the RqHAuth, it verifies if the value of the NewT is in the acceptable range according to the time synchronization configuration, if yes goto next step if not reject the handover request. Then, it computes the new privates key to decrypt the message, $SKAPnew = g^{h(Rw^*||IAPnew)} \bmod p.$ The APnew checks also the session_id with the SessK, if the NewT, Iu and Session_id are valid, the APnew sends a response handover authentication message (ResHAuth) within Rw* and the decrypted value of the random number RIu*.

$$AP \rightarrow \neq wU: ResHAuth,$$
$$ResHAuth = (RIu^*, Rw^*)_{K_{APnew}},$$

where, $KAPnew = g^{h(Rw^*||NewT)} \bmod p.$

After receiving the ResHAuth, the device user verifies the legitimacy if the new accesspoint by IAPnew and RIu* if yes,

the handover authentication protocol enable the mobility communication between the entities. The data communication is encrypted by $SessK^* = H(RIu^* \| Rw^*)$. This is the end of the handover authentication protocol.

IV. Security Analysis

This section discuss about the security analysis of the proposed protocol. This protocol presents the requirements performance for the security. Data integrity and confidentiality are provided by the public key encryption and replay attack is prevented by the time stamp usage with Current and New Time for each session.

V. Conclusion

This section discuss about the security analysis of the proposed protocol. This protocol presents the requirements performance for the security. Data integrity and confidentiality are provided by the public key encryption and replay attack is prevented by the time stamp usage with Current and New Time for each session.

References

1] IEEE 802.11b, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-speed Physical Layer Extension in the 2.4 GHz Band,” *IEEE Standard*, September1999.

[2] IEEE 802.11a, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHz Band,” *IEEE Standard*, September1999.

[3] IEEE 802.11g, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Further Higher-Speed Physical Layer Extension in the 2.4GHz Band,” *IEEE Standard*, June2003.

[4] IEEE 802.11g, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Further Higher-Speed Physical Layer Extension in the 2.4GHz Band,” *IEEE Standard*, June2003.

[5] J. Bray and C. F. Sturman, *Bluetooth 1.1 Connect Without Cables*. Prentice Hall, 2002, ISBN: 0-13-066106-6.