M2M 통신에서 원격장치 인증 기법

이송희*, 박남섭**, 이근호***

A remote device authentication scheme in M2M communications

Song-Hee Lee*, Nam-Sup Park, Keun-Ho Lee*****

요 약 사물지능통신(Machine to Machine) 은 사람의 도움없이 언제, 어디서나 독립적으로 기기간 통신을 가능하게 한다. M2M통신은 보통 무선구간의 통신을 포함하므로 도청, 가로채기, 변조, 프라버시 침해 등의 보안문제가 많이 발생할 수 있다. 따라서 무엇보다 기기들간의 안전한 통신을 이루는 것이 가장 중요한 문제 중 하나이다. 본 논문에서는 M2M 아키텍처에서 M2M 도메인과 네트워크 도메인간에 인증을 통해 데이터 노출을 피하고 안전한 통신을 제공하기위해 동적 ID기반의 원격 인증 기법을 제안한다. 제안된 기법은 로직기반의 정형검증을 통해서 우수한 보안성과 안전성이 증명되었다.

주제어 : 사물지능통신, 원격 인증, 동적 ID, 정형기법

Abstract Machine-to-machine (M2M) communication occurs when devices exchange information independent of human intervention. Prominent among the technical challenges to M2M communication are security issues, such as eavesdropping, spoofing, modification, and privacy violation. Hence, it is very important to establish secure communication. In this paper, we propose a remote authentication scheme, based on dynamic ID, which provides secure communication while avoiding exposure of data through authentication between the M2M domain and the network domain in the M2M architecture. We then prove the correctness and security of the proposed scheme using a logic-based formal method.

Key Words : M2M, Remote authentication, dynamic ID, formal method

1. Introduction

Machine-to-machine (M2M) communication has emerged as one of the next frontiers in wireless communications. It is now undergoing rapid development and continues to inspire many new applications [3][12][15]. In M2M communication, devices can exchange information with each other autonomously, i.e., without requiring human intervention [7][15]. M2M communication systems apply to a wide variety of sectors including manufacturing, healthcare, transportation, logistics, security, and IT/networking, and generally to any technical enterprise that seeks to improve efficiency and lower costs. In addition, M2M supports communication among the burgeoning numbers of heterogeneous smart devices. For these reasons, M2M has become an indispensable component of next generation networks, e.g., the Internet of Things (IoT)[1][7]. However, the flourishing of M2M communication hinges on fully understanding and managing existing technical challenges, such as energy efficiency, reliability, and security. Indeed, the lattermost of these concerns, security, poses a distinct challenge to widespread adoption, given the ubiquity and autonomous nature of M2M communications[4][14].

*한국인터넷진흥원 선임연구원
**LG전자 책임연구원
***백석대학교 정보보호전공 교수(교신저자)
논문접수: 2013년 1월 26일, 1차 수정을 거쳐, 심사완료: 2013년 2월 14일, 확정일: 2013년 2월 20일

Recently, a number of efforts have been made toward the standardization of M2M communications[9]. Most of these standards have moved quickly to propose the architectural and air interface modifications required by M2M communication systems. Unfortunately, since research on security issues in M2M communication is still in its infancy [5], little progress has been made toward a coherent security standard.

The data collected and handled by M2M devices is typically sent to a back-end server through the wireless network, which is very dangerous. To guarantee security of information, an M2M communication must provide for closed and well-defined communications between the M2M domain and the network domain. In addition, the complexity of the security should not be complicated.

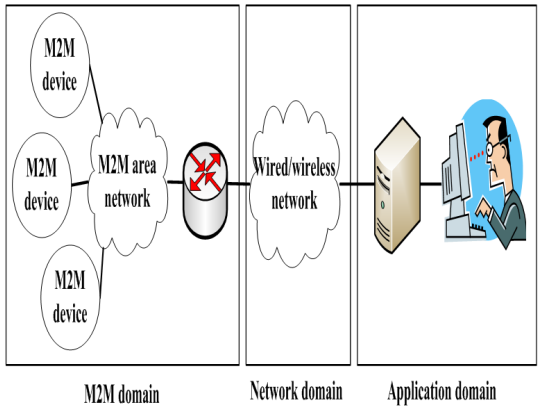
In this paper, we propose a remote device authentication scheme that meets these criteria. Our scheme, based on dynamic ID, uses only simple operations such as a one-way hash function and a bitwise exclusive OR operation. We then provide a security analysis of our scheme as well as a formal analysis using logic-based formal methods.

2. Related Work

As shown in Fig. 1, an M2M communication architecture comprises an M2M domain, a network domain, and an application domain. Generally, M2M devices intelligently collect monitoring data inside the M2M domain, while the wired/wireless network relays the collected data to a back-end server, which may support numerous M2M applications within the application domain[14].

The research on security issues in M2M communication is still inadequate [9]. Most of recent research serves to outline only potential security threats and security requirements for M2M communication systems [3][4][5][9][14].

According to previous research, M2M communication systems are extremely vulnerable to attacks for several reasons. First, they are especially open to physical attack because M2M devices operate autonomously, without human intervention. Second, M2M devices mainly communicate with each other in a wireless environment, which makes eavesdropping very easy. Finally, M2M devices are typically characterized by low energy use and minimal computing resources [5][9].



[Figure 1] Simple M2M communication architecture

3. Proposed authentication scheme

In this section, we describe our remote device authentication scheme for use between M2M and network domains. We assume that an M2M device has a smartcard personalized from a remote server in the application domain. A detailed illustration of this scheme is given in Fig. 1. The notation we use to describe our scheme and cryptographic operations is given in Table 1.

There are four phases within our scheme: the registration phase, login phase, verification phase, and password change phase. Tasks contained in these phases are described as follows:

〈Table 1〉 Notation

Notation	Description
D_i	M2M device i
ID_i	Identity of D_i
PW_i	Password of D_i
BS	Remote server
x	Permanent secret key of S
h(.)	A cryptographic one-way hash function
⇒	A secure channel
→	A common channel
	A bitwise exclusive-OR exclusion operation

3.1 Registration phase

An M2M device D_i sends a registration request to the remote server BS over a secure channel:

① D_i chooses a random number r and a password PW_i to compute $R_i=h(r||PW_i)$ and $HID_i=h(ID_i||r)$
② D_i submits R_i and HID_i to BS.
③ The remote server BS computes $DID_i=h(HID_i||x)$ where x is secret to the server. The sever BS issues a smartcard containing security parameters [h(.), DID_i,x].
④ D_i computes $N_i=r\oplus h(ID_i||PW_i)$ and inserts N_i in its smartcard. The smartcard now stores the necessary security parameters (h(.),DID_i,x,N_i) in its memory.

3.2 Login phase

When the device wants to login to the remote server to send sensory data, the device accesses the smartcard to log on to the remote server BS and submits its ID_i and password PW_i. The smart card computes $DID'=h(h(ID_i)||x)$ and compares it with the stored value of DID_i in its memory to verify the device. The smart card then performs the following steps:

① The smart card checks if $DID_i'?=DID_i$. If so, then ID_i is a valid device's ID and further operations may proceed, otherwise they are terminated. After identity verification, the smart card computes a session ID: SID_i = h(DID||T),where T is the current date and time of input device. Then the smartcard computes $r=N_i\oplus h(ID_i||PW_i)$,$R_i=h(r||PW_i)$, and $M_i=N_i\oplus H(R_i||T)$.
② D_i sends the computed values SID_i, M_i, and T to the BS.

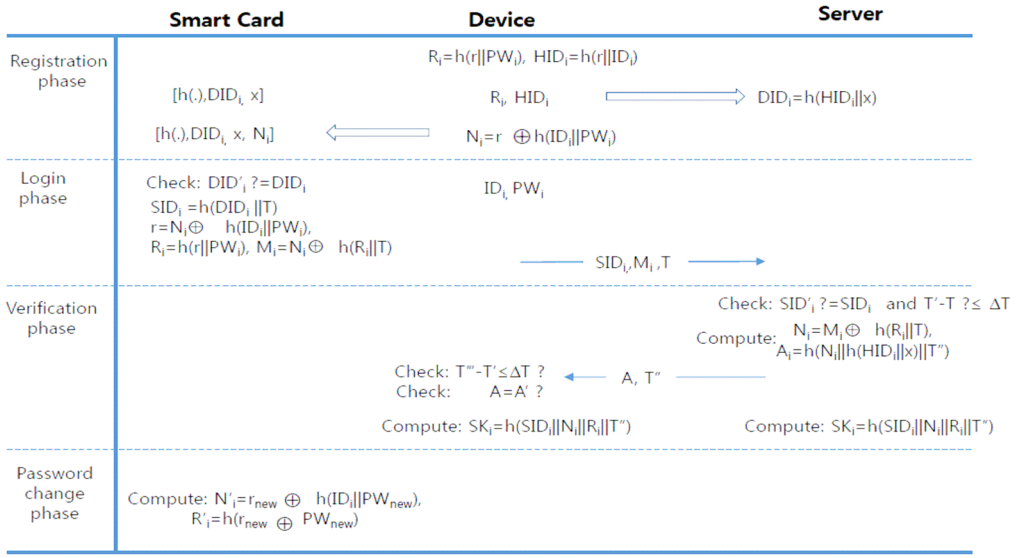
3.3 Verification phase

In this phase, the remote server BS verifies the authenticity of the login message requested by the device Di. The remote server BS performs the following steps:

① Upon receiving the message (SID_i,M_i,T), BS checks the validity of ID and the freshness of T. The validity of IDis checked by performing $SID_i?=SID_i'$, where SID_i' can be computed by $SID_i'=h(h(HID_i||x)||T)$. If they are equal, then ID_i is a valid device's ID, and further operations may proceed; otherwise, the login request is refused. The freshness of T is checked by performing $T'-T\leq\Delta T$, where T' is the current date and time of the remote server BS and ΔT is the expected time interval for a transmission delay. If ΔT is a valid time interval, BS accepts the login request of D_i; otherwise, the login request is refused.
② BS computes $N_i=M_i\oplus H(R_i||T)$ and $A_i=h(N_i||HID||x||T'')$, where T'' is the current date and time of the remote server BS.
③ BS sends the computed values A and T'' to D_i.

3.4 Password change phase

When the device wants to change its password, it sends a request to change the password PW_i to a new one, say PW_{new}, and the smartcard then computes $N'_i=r_{new}\oplus h(ID_i||PW_{new})$ where r_{new} is a new random value, and $R'_i=h(r_{new}\oplus PW_{new})$. N_i now reflects the new password PW_{new}.



[Figure 2] Device authentication scheme between M2M domain and application

4. Security analysis

In this section, we compare the security of our proposed scheme with that of Wang et al., and demonstrate that our scheme provides better overall security strength.

First, we note that our scheme employs only a dynamic session ID (SID) for login processing, unlike Wang et. al's use of a static one. Our SID changes whenever a new session is created. Hence, our scheme avoids the risk of ID theft and preserves user anonymity.

Second, Wang et. al's scheme cannot protect against insider attacks from the remote server because the remote server knows each user's ID and password and may therefore function as an insider adversary. In our scheme, the device chooses its own password and computes the hash value of this password combined with a random number, as well as the hash value of device's ID.

The device then submits these hash values to the remote server. Thus, the remote server cannot deduce the ID and password of the device, virtually removing the threat of an insider adversary.

Third, although an adversary can extract the secret information stored on the device's smartcard by monitoring the power consumption or analyzing the leaked information, our scheme nevertheless resists offline password guessing attacks. For example, an adversary may obtain DID_i, x, as well as N_i from the smartcard, and supposing the adversary also intercepts one of device's past login messages(i.e.,$\{SID_i,M_i,T\}$), he or she can try to guess the password of the user, and there by induce $h(R_i||T)$ from Mi ⊕ Ni.

However, he cannot know the Ri and so cannot guess the password of the device. This aspect of our proposed scheme effectively prevents offline password guessing attacks.

Finally, supposing once again that the adversary has intercepted one of the device's previous login messages (i.e. $\{SID_i,M_i,T\}$). To impersonate a validated device D_i and login BS at time T ′ (>T), the adversary must also compute the valid message SID_i, M_i T. However, he or she cannot compute both the SID_i and M_i, because the hash value $H(R_i||T)$ uses a concatenation of the validated device's time T, and the gap between

the invalid time and the current time of adversary's clock is detectable. Hence, there mote server BS cannot proceed to the next process. Therefore, our scheme is resistance to the impersonation attack.

5. Formal analysis

In this section, we describe our formal analysis of mutual authentication between an M2M device and a remote server based on logic[15−16]. GNY logic is mainly used to analyze the security of cryptographic schemes. All symbols, notations, and rules are cited in[15−16].

We formalize the login phase and the verification phase to verify the mutual authentication between an M2M device and a remote server as follows:

Msg1. $BS \lhd (*h(h(HID_i \| x) \| T), *(N_i \oplus h(R_i \| T)), *T)$

Msg2. $Device \lhd (*h(N_i \| HID_i \| x \| T''), *T'')$

We also make the following initial assumptions about our scheme:

($A1$) $BS \ni x$

($A2$) $BS \ni HID_i,\ R_i$

($A3$) $BS \mid\equiv \#(T''),\ \#(T)$

($A4$) $Device \ni h(HID_i \| x),\ R_i,\ N_i$

($A5$) $Device \mid\equiv \#(T),\ \#(T'')$

These assumptions describe the possessions and beliefs of the remote server and the M2M device. Assumption (A1) indicates that the remote server possesses its own secret value x. Assumption(A2) indicates that the remote server knows the hashed values HID_i, R_i, and N_i. Assumption (A3) indicates that the remote server believes that timestamp T'' is fresh. Assumption (A4) indicates that the M2M device possesses and knows the hashed values $h(HID_i \| x)$, R_i, and N_i. Finally, assumption (A5) indicates that the M2M device believes that timestamp T'' is fresh.

Msg1 yields the following equations by applying rules .

$$\frac{BS \lhd (*h(h(HID_i \| x) \| T),\ *(N_i \oplus h(R_i \| T)),\ *T)}{BS \lhd h(h(HID_i \| x) \| T),\ (N_i \oplus h(R_i \| T)),\ T} \quad (1)$$

Applying rules P1, P3, and P5, we obtain

$$\frac{BS \lhd h(h(HID_i \| x) \| T),\ (N_i \oplus h(R_i \| T)),\ BS \ni R_i,\ BS \ni T}{BS \lhd h(h(HID_i \| x) \| T),\ BS \ni N_i,\ BS \ni h(R_i \| T)} \quad (2)$$

Applying assumptions (A1) and (A2) and rule P4, we obtain

$$\frac{BS \lhd h(h(HID_i \| x) \| T),\ BS \ni HID_i,\ BS \ni x,\ BS \ni T}{BS \ni h(h(HID_i \| x) \| T)} \quad (3)$$

Applying assumptions (A1) and (A2) and rules P2 and R6, we obtain

$$\frac{BS \ni h(h(HID_i \| x) \| T),\ BS \ni N_i,\ BS \ni h(R_i \| T),\ BS \ni T}{BS \mid\equiv \varphi\ (h(HID_i \| x) \| T),\ BS \mid\equiv \varphi\ T,\ BS \mid\equiv \varphi\ (N_i \oplus (R_i \| T))} \quad (4)$$

Applying assumptions (A1) and (A2), rules R1 and R5, and Equation (4), we obtain

$$\frac{BS \mid\equiv \varphi\ (h(HID_i \| x) \| T),\ BS \mid\equiv \varphi\ (N_i \oplus (R_i \| T))}{BS \mid\equiv \varphi\ h(h(HID_i \| x),\ BS \mid\equiv \varphi\ (N_i),\ BS \mid\equiv \varphi\ (R_i \| T)} \quad (5)$$

Applying assumptions (A1), (A2), and (A3), rule F10, and Equation (3), we obtain

$$\frac{BS \mid\equiv \#(T),\ BS \ni T}{BS \mid\equiv \# h(h(HID_i \| x) \| T),\ BS \mid\equiv \#(N_i \oplus h(R_i \| T))} \quad (6)$$

The remote server possesses timestamp T and its own secret value x, and can thus compute the hashed

values $h(h(HID_i \| x) \| T)$, $h(R_i \| T)$, and N_i, as shown in Equations (1 - 3). It also believes in the freshness of Msg1., because the message is generated during the current run of the scheme and hence cannot be a replay of a message from previous runs. The remote server further believes that the M2M device Di conveyed the message by identifying the dynamic ID HID_i in Msg1., described as follows: $BS \equiv Device \sim Msg1$. The remote server can then generate the hashed value A = $h(N_i \| HID_i \| x \| T'')$.

Msg2 yields the following equation by applying rules T1 and T2.

$$\frac{Device \lhd (*h(N_i \| h(HID_i \| x) \| T''),\ *T'')}{Device \lhd h(N_i \| h(HID_i \| x) \| T''),\ T''} \quad (7)$$

Applying assumption (A4) and rules P1, P3, and P4, we obtain

$$\frac{Device \ni N_i,\ Device \ni h(HID_i \| x),\ Device \lhd T''}{Device \ni h(N_i \| HID_i \| x \| T''),\ Device \ni T''} \quad (8)$$

Applying assumption (A4) and rules P2 and R6, we obtain

$$\frac{Device \ni h(N_i \| h(HID_i \| x) \| T''),\ Device \ni h(HID_i \| x),\ Device \ni T''}{Device \equiv \varphi(N_i \| h(HID_i \| x) \| T),\ Device \ni T''} \quad (9)$$

Applying assumption (A4), rules R1 and R5, and Equation (9), we obtain

$$\frac{Device \equiv \varphi(N_i \| h(HID_i \| x) \| T),\ Device \ni T''}{Device \equiv \varphi\ h(N_i \| h(HID_i \| x) \| T),\ Device \ni T''} \quad (10)$$

Applying assumptions (A4) and (A5), rule F10, and Equation (8), we obtain

$$\frac{Device \equiv \#(T''),\ Device \ni T''}{Device \equiv \# h(N_i \| h(HID_i \| x) \| T)} \quad (11)$$

The M2M device possesses timestamp T'' and the hashed values $h(N_i \| h(HID_i \| x) \| T'')$, $h(HID_i \| x)$, R_i, and N_i, as shown in Equations (7) and (8). The M2M device computes the hashed values $h(N_i \| h(HID_i \| x) \| T'')$, $h(HID_i \| x)$, R_i, and N_i and believes that Msg2 is fresh. Since only the remote server and the smartcard know the hashed value $h(HID_i \| x)$, the M2M device believes that the remote sever conveyed Msg2, as follows: $Device \equiv BS \sim Msg2$. Thus, the remote server and the M2M device can generate the same session key $SK_i = h(SID_i \| N_i \| R_i \| T'')$ and mutually authenticate that key as follows:

$$BS \equiv Device \equiv BS \xleftrightarrow{SK_i} Device$$

and

$$Device \equiv BS \equiv Device \xleftrightarrow{SK_i} BS$$

.

6. Conclusions

In M2M networks, devices can autonomously communicate with each other without any human intervention. However, M2M communication systems are attractive targets to attackers, as collected data can be easily disclosed.

In this paper, we proposed a remote device authentication scheme that is significantly more secure than previously proposed schemes. We demonstrated that this scheme is resistant to ID theft, insider attacks, offline password guessing attacks, and impersonation attacks. In addition, we proved the correctness and security of the proposed scheme using the GNY logic-based formal method.

Acknowledgement

"This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(grant number) "(No.2012-0003141)"

References

[1] Booysen. J, Gilmore. S, Zeadally. S, Rooyen. J. (2011). Machine-to-machine (M2M) communications in vehicular networks. KSII Transactions on Internet and Information Systems, 6(2): 529－546.

[2] Burrows. M, Aba. M, Needham. R. (1990). A logic of authentication [J]. ACM Transactions on Computer Systems, 8(1): 18－36.

[3] Cha. H, Shah.Y, Schmidt. U, Leicher. A, Meyerstein. V. Trust in M2M communication [J]. IEEE Vehicular Technology Magazine, 2009, 4(3): 69－75.

[4] Chen. D, Chang. G. (2012). A survey on security issues of M2M communications in cyber-physical systems. KSII Transactions on Internet and Information Systems, 2012, 6(1): 24－45.

[5] Chen. H, Fu. Z, Zhang.D, (2011). Security and trust research in M2M system [C]// Proceedings of the 7th Annual Conference of the IEEE Intelligent Transportation Systems Society. Beijing, 286－290.

[6] Das. L, Saxena. A, Gulati. P. (2004). A dynamic ID-based remote user authentication scheme [J]. IEEE Transactions on Consumer Electronics, 50(2): 629－631.

[7] Geng. W, Talwar. S, Johnsson K, Himayat. N, Johnson. D. (2011). M2M: From mobile to embedded internet IEEE Communications Magazine, 49(4): 36－43.

[8] Gong. L, Needham. R, Yahalom. R. (1990). Reasoning about belief in cryptographic protocols[C]// Proceedings of the IEEE symposium on Research in Security and Privacy, Oakland, 234－248.

[9] Jorge. G, Edmundo. M. (2012). Security in M2M environments . WiNeMO White Paper, 3－6.

[10] Ku. C, Chen. M. (2004). Weaknesses and improvements of an efficient password based remote user authentication scheme using smartcards [J]. IEEE Transactions on Consumer Electronics, 50(1): 204－207.

[11] Lamport. L (1981). Password authentication with insecure communication [J]. Communications of the ACM, 24(11): 770－772.

[12] Lawton G. (2004). Machine-to-machine technology gears up for growth [J]. IEEE Computer, 37(9): 12－15.

[13] Liao. I, Lee. C, Hwang. S. (2005). Security enhancement for a dynamic ID based remote user authentication scheme [C]// Proceedings of the 5th Annual Conference of the International Conference on Next Generation Web Services Practices. Washington D.C, 437－440.

[14] Lu. R, Li. X, Liang. X, Shen. X, Lin. X. (2011). The green, reliability, and security of emerging machine-to-machine communications. IEEE Communication Magazine, 49(4): 28－35.

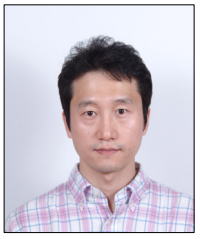
[15] Niyato. D, Lu. X, Wang. P. (2011). Machine-to-machine communications for home energy management system in smart grid IEEE Communications Magazine, 49(4): 53－59.

[16] Wang. Y, Liu. Y, Xiao. X, Dan. J. (2009). A more efficient and secure dynamic ID-based remote user authentication scheme [J]. Computer Communications, 32(4): 583－585.

이 송 희

・2009년 2월 : 고려대학교 컴퓨터학과 (이학박사)
・2009년 9월 ~ 2012년 11월 : 고려대학교 융합소프트웨어 연구소 연구교수
・2012년 11월 ~ 현재 : 한국인터넷진흥원 선임연구원
・관심분야 : 네트워크보안, 소프트웨어 보안, 정형검증
・E-Mail : shlee@kisa.or.kr

박 남 섭



・2006년 8월 : 고려대학교 컴퓨터학과 (이학박사)
・2006년 3월 ~ 현재 : LG전자 MC연구소 책임연구원
・관심분야 : 멀티미디어 통신, 모바일 통신, 네트워크 보안
・E-Mail : namsup.park@lge.com

이 근 호

・2006년 8월 : 고려대학교 컴퓨터학과 (이학박사)
・2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
・2010년 3월 ~ 현재 : 백석대학교 정보통신학부 조교수
・관심분야 : M2M 보안, 이동통신 보안, 융합 보안, 개인정보 보호
・E-Mail : root1004@bu.ac.kr