A Dynamic ID-Based Authentication Scheme for M2M Communication of Healthcare Systems

Tien-Dung Nguyen and Eui-Nam Huh
Department of Computer Engineering, Kyung Hee University, Korea

Abstract: *Machine to Machine (M2M) applications involving intelligence to ubiquitous environment have been in existence for the past many years. However, its provisioning using mobile technologies raises a new security challenge. Security services such as authentication and key establishment are critical in M2M, especially for healthcare systems. We proposed a simple architecture M2M service to apply any hospital which considers mobility of doctors and patients. An efficient security scheme with dynamic ID-Based authentication using pairwise key distribution is applied in M2M system. It can be assured high security through security analysis under shared key attack and sybil attack.*

Keywords: *M2M, u-healthcare, WSN, authentication.*

Received March 24, 2010; accepted October 24, 2010

1. Introduction

Today, mobile operators in developed markets are actively seeking new avenues for revenue generation since the traditional sources such as voice are getting saturated. Machine to Machine (M2M) communication is considered as one such opportunity. M2M is defined differently in literatures and contexts. A broader definition of M2M communication includes the remote control of machines telematics and monitoring collecting data from machines telemetry. Recently, from a mobile perspective, M2M is defined as communication between a machine and a mobile terminal (machine-to-mobile and mobile-to-machine) or between a machine and a back-end information system (machine-to-machine). M2M application is basically related to Wireless Sensor Network (WSN) by combining mobile devices and sensor nodes. Application of sensor for analyzing diversified context information is rising. In the case of healthcare services, changes in action and context of patient must be responded sensitively. It is difficult for staffs, nurses or doctors to check context of patients every time and it becomes more difficult to detect these changes when the patient is in different places. Therefore, the study is suggesting a context-aware system for checking health context of patients. By centering on patients whom require continuous monitoring, temperature, heartbeats, etc., will be collected by sensors for measuring basic metabolism. In addition, information such as temperature, humidity, etc., will be collected for analyzing living pattern of the patient as shown as Figure 1. By using mobile devices (PDA), doctors, nurses and medical staffs can manage such information in real-time without geographical barriers easily and quickly. Some recent u-healthcare applications also solve these issues such as monitoring the context of patients by bio-sensors and PDA through Ethernet WiFi etc., or mobile communication system 3G, CDMA etc. These applications bring not only to doctors, nurses, staffs but all patients as well a huge advantage. However, these solutions often support for the big applications which need communication servers, authentication servers, and many middle devices to transfer data from sensors to internet. Therefore, the total cost is very expensive. In order to reduce this cost, M2M service is a desirable solution. Mobile devices e.g., PDA only need to communicate with sensor nodes directly to receive all information of other sensor nodes. By applying this simple M2M application, it brings lots of benefits to patients and doctors. Doctors, nurses and medical staffs can manage such information in real-time without geographical barriers, and patients can receive careful monitoring from them anytime. To implement this M2M application, the middle devices between sensor and gateway or sensor and mobile device are not use. Communication will base on wireless sensor network; mobile devices will communicate with sensor nodes to gather all information. Thus, this is the most convenience way for doctors to communicate with patients.

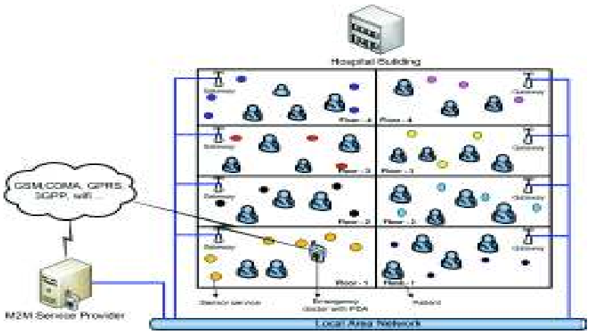


Figure 1. M2M application in hospital.

Nevertheless, security problem is the most important in this scenario, how authentication scheme can protect the confidential information of all patients. Without the secure service, M2M is very dangerous as sensing data can be easily disclosed to anybody. In this paper, we propose an authentication scheme that prevents the communication between doctors (mobile devices) and patients (sensor nodes) from attacking of illegitimate users.

2. Related Work

Mobile to Machine (M2M) system consists of thousand of sensors and mobile which traverses the network using random walk. By arming with built-in sensor, mobile device can communicate with wireless sensor network easily. Therefore, in order to create a new efficient security mechanism for M2M system, previous research reports related to security in WSN are reviewed.

In this section, previous research reports related to key management and authentication in WSN security are reviewed. Eschenauer and Gligor (EG) [6] proposed the basic probabilistic key pre-distribution where each node stores a random subset of keys from a large key pool before deployment. As a result, two nodes have a certain probability to share at least one key after deployment. Chan *et al.* [4] extended this scheme to enhance the security and resilience of the network significantly by requiring at least two common shared keys for authenticated communication and updating communication keys for subsequent communications. The communication is authenticated with a key in these schemes but node identities are uncertain; thus, Chan *et al.* [3] further advocate a random pair wise key scheme PIKE that allows only two nodes to share the value of a particular key and supports key revocation by either a base station or neighboring nodes. The disadvantage of PIKE is it requires the trust from the third intermediary nodes for authentication.

Watro *et al.* [20] developed the TinyPK system that requires each node to be preloaded with a static Diffie-Hellman key pair and a node identity string processed by a Certificate Authority's private key allowing node authentication. Perrig *et al.* [13] propose the SPINS Secure Network Encryption Protocol (SNEP) and the μTimed, Efficient, Streaming, Losstolerant Authentication (μTESLA) components as building blocks for securing sensor networks. The SNEP component offers semantic security with an incremented counter that causes a different encryption result for the same message content, a Message Authentication Code (MAC) for verification of sending and receiving nodes, replay protection, and weak assurance of data freshness via use of the encrypted counter. The μTESLA component associates symmetric key release to a particular time interval; thus allowing recognition and denial of a spoofed packet using a key after time interval expires.

Du *et al.* [5] (DDHV, DDHV-D), [8, 9, 10, 12, 21] utilize deployment knowledge to improve the probability of the key sharing and enhance the resistance to node capture. Carman [2] combined the benefits of both identity-based cryptography and random key pre-distribution into ID based authentication framework for wireless sensor network. A survey of key management in ad hoc networks is given in [7]. The latest survey of security issues for WSNs is presented in [18, 19].

Rasheed and Mahapatra [14] exploit the use of two different key pre-distribution schemes in conjunction to establish a secure link between a mobile sink and a sensor node. Besides, Rasheed and Mahapatra [15] also proposed a novel countermeasure attack for sensor networks with controlled mobility. But the proposed security mechanism does not apply to sensor networks that use a mobile sink with random walk to gather sensors data. The proposed scheme uses a dynamic ID-based authentication using pairwise key pre-distribution to establish a pairwise key between mobile sink and any sensor node. Since sensors are hardware- and power-limited, we consider computationally efficient methods, such as the use of an efficient hash function, to prevent attacks on the network. The proposed security mechanism uses a dynamic ID-Based authentication with Blom's scheme [1] and collision-resistant hash function, such as MD5 [16], to authenticate the source of the beacon signal before sensor nodes are allowed to transmit their aggregated data to the trusted mobile sink.

3. Proposed Security Scheme

3.1. Notation

We use the following notation in Table 1 to describe security protocols and cryptographic operations in this paper.

Table 1. Notation.

Notation	Description
M	Mobile M (user)
$\mathbf{K_m}$	Master key
IPM	Address of M to M2M service.
$\mathbf{ID_m}$ $\mathbf{\{ID_{m2m}\Vert ID_M\}}$	Identify of mobile M {Id of M2M service || # Id of mobile M}
$\mathbf{ID_a\ \{ID_{G1}\ \Vert ID_A\ \}}$	Id of node A {Identify of domain 1|| # id of node A}
Nonce	Nonce is an unpredictable bit string
$\mathbf{K_{M2M}}$	Secret (Symmetric) key between Mobile and M2M Service Provider
$\mathbf{K_{bm}}$	Shared key between node b and m
S	Key space
$\mathbf{ID_1\Vert ID_2}$	The concatenation of ID_1 and ID_2
$\mathbf{MAC(K_1,[M])}$	Encryption of message M with K_1 using CBC MAC [13]
E([M],K)	Encryption of message M with the symmetric key K
ω	Total number of key spaces
τ	Number of key spaces in ω
λ	Number of compromised node
$\mathbf{A^T}$	The transpose of matrix A
$\mathbf{A \cdot B}$	The product of matrix A and B

3.2. Architecture of Health Monitoring Application

We assume regular stationary sensor nodes are constrained in resources, and the mobile device moves along a random path to gather sensor data. A mobile device can be as powerful as a laptop-class device or a PDA with external device or built-in sensor node that can communicate with wireless sensor network. Routing table of each sensor will be updated automatically when mobile (doctor) traverses. Each domain has same protocol and key spaces.

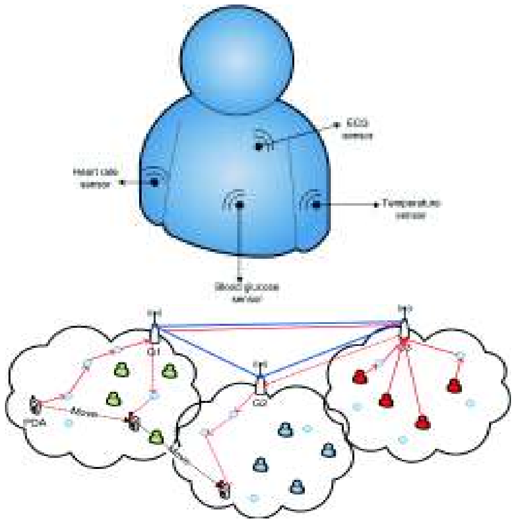


Figure 2. Mobile user monitors all patients in domain 3.

Figure 2 describes some patients may need to test some medical in other room (domain 3). Although doctor stays in room (domain 1), he wants to know his patient's context. In this case, our application will help doctor can monitor all his patients anytime. The problem of this scenario is mobility of doctors and patients. Doctor uses mobile devices which can be as powerful as a laptop-class device or PDA while patients are integrated with sensors which are hardware and power limited. Therefore, one proposed security scheme has to satisfy these conditions.

The idea of our proposed security scheme is ID-based, using ID as a secret key in system to authenticate each other. In order to implement this security scheme, we assume the system includes many domains in which have one or more rooms on the same floor. Each domain has one gateway, static sensor nodes and mobile sensor nodes as shown as Figure 3. A gateway has same function with coordinator and can communicate with other gateways. The mission of gateway is manage information of all sensor nodes in domain that help doctor can monitor all patients easily. Static sensor nodes which are placed in each room to measure temperature, humidity…, and mobility sensor nodes are sensor nodes which are integrated in patients as Figure 2 shown. Architecture of gateway is composed of four parts: query dissemination, data aggregation, security, and routing. Query dissemination part is called out-communication part. When a doctor requests a service that consists of context of patients in other domain, gateway will use this part to query from other gateways. Data aggregation part will collect, manage all data in his domain include patients. Normally, data aggregation part will update database automatically. Security part is the important part that supplies security mechanism to all sensor nodes in domain. The last part is routing part that control routing processing in domain. Besides, model of static sensor and mobile sensor are quite similar, they consist of data gathering function to collect information from environment or patient's context and routing function to update routing table to neighbor nodes. Especially, static sensor has own M2M service function to supply service for doctor who want to monitor patients. The communications of each function from gateway to sensor nodes are described in Figure 3.

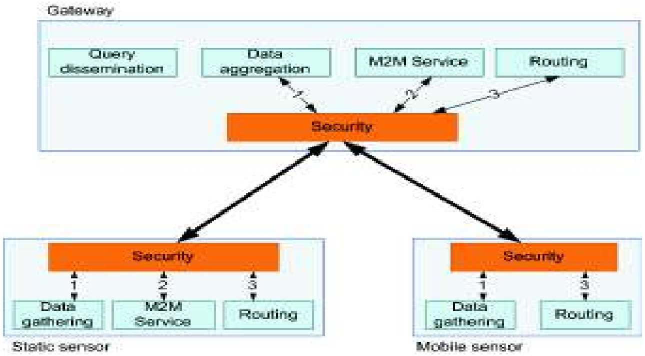


Figure 3. Domain model.

M2M service is described by 6 steps as Figure 4 shown:

- *Step 1:* Mobile phone (doctor) uses M2M service to send request to static sensor node.
- *Step 2:* Static sensor node sends request to Gateway.
- *Step 3:* After receiving request from static sensor, M2M Service part in gateway transfers request to Query dissemination part.
- *Step 4:* Base on request, query dissemination part will collect data inside domain from data aggregation or collect data outside domain from query dissemination part in other gateways.
- *Step 5:* Query dissemination part stores data in buffer and transfer them to M2M Service in gateway consequently. Then, base on routing information, M2M Service responses data to static sensor which is closest with mobile phone.
- *Step 6:* In static sensor, M2M Service forwards data to mobile phone.

During data processing, gateways update routing information and aggregate data from mobile sensors (patients) regularly. *<ID, name, info>* is structure of data dissemination in which *info* element shows the services of M2M application included statuses corresponding with sensors on patients: heart rate, ECG (Electrocardiogram), temperature and blood glucose. Base on this information, doctor can use the suitable therapeutic method.

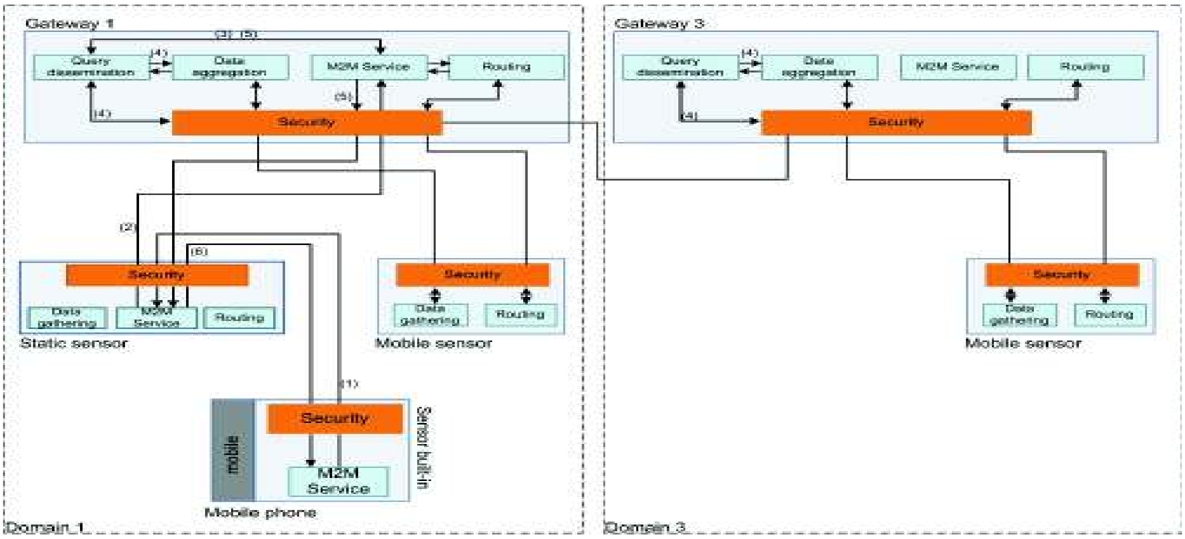


Figure 4. Architecture system model for M2M service.

3.3. ID Set-Up Phase

In this phase, Identity (ID) is initialized in all sensors and gateways in network as ID-based authentication. Because our system is distributed to many domains, each domain has many sensors and one gateway. Therefore, ID of each sensor will be concatenated by ID of domain *(ID_d)* and ID of unique sensor *(ID_s)* or ID of gateway (filled with all 0). By this way, ID of sensor x in domain x is *$[ID_{dx}||ID_{sx}]$*, and ID of gateway x is *$[ID_{dx}||0]$*. On the other hand, mobile devices have also identity *$[ID_{m2m}||ID_m]$*, with ID_{m2m} is the identity number of M2M service which differ from ID of other domains. Besides, each static sensor stores all ID of his neighbors in the same domain, list of ID_d and ID_{m2m}. Mobile sensors just store all ID of neighbor static sensors in same domain. Gateway stores all ID of sensors static and mobile sensors, ID of other gateways and M2M service identity (ID_{m2m}).

3.4. Pre-Distribution Phase

3.4.1. Pre-Distribution for Network System

Probabilistic key management framework [12] will be applied to our scenario. During the key pre-distribution phase, we need to assign key information to each node, such that after deployment, neighboring sensor nodes can find a secret key between them. As concerned in ID set-up phase, that each sensor node has a unique identification, whose range is from *1* to *N* for each domain. In pre-distribution phase, ω denotes the total number of key spaces and τ denotes the number of key spaces in ω spaces which are used to authenticate between nodes $(2 \leq \tau < \omega)$. As long as no more than λ nodes are compromised, the network is perfectly secure (this is called the λ-secure property). These parameters decide the security and performance of our scheme, and will be discussed later in the paper. Our key pre-distribution phase for each domain contains the following steps:

1. *Step 1 Generating G Matrix:* We first select a primitive element from a finite field *GF(q)*, where *q* is the smallest prime larger than the key size, to create a generator matrix *G* of size $(\lambda+1)\times N$. Let *G(j)* represent the j^{th} column of *G*. We provide *G(j)* to node *j*. Each sensor only needs to remember one seed (the second element of the column), which can be used to regenerate all the elements in *G(j)*. Therefore the memory usage for storing *G(j)* at a node is just a single element. Since the seed is unique for each sensor node, it can also be used for node id.
2. *Step 2 Generating D Matrix:* We generate ω symmetric matrices $D1,\ldots,D_\omega$ of size $(\lambda+1)\times(\lambda+1)$. We call each tuple $S_i=(D_i,G)$, $i=1, \ldots, \omega$, a key space. We then compute the matrix $A_i=(D_i.G)^T$. Let $A_i(j)$ represent the *j*th row of A_i.
3. *Step 3 Selecting τ Spaces:* We randomly select τ distinct key spaces from the ω key spaces for each node. For each space S_i selected by node *j*, we store the j^{th} row of A_i (i.e., $A_i(j)$) at this node. This information is secret and should stay within the node; under no circumstance should a node send this secret information to any other node. According to Blom's scheme [1], two nodes can find a common secret key if they have both picked a common key space.

For example: Initially node *i* has $\{A_x(i),\ldots,A_y(i)\}$ with key spaces $\{S_x,\ldots S_y\}$ and seed for *G(i)*, and node *j* has $\{A_a(j),\ldots,A_b(j)\}$ with key spaces $\{S_a,\ldots S_b\}$ and seed for *G(j)*. Two nodes want to communicate, and then node *i* will send key space S_c to node *j*. If key space S_c exists in node *j*, then they try to exchange the seeds, node *i* can regenerate *G(j)* and node *j* can regenerate *G(i)*; then the pairwise secret key between nodes *i* and *j*, $K_{ij}=K_{ji}$, can be computed in the following manner by these two nodes independently: $K_{ij}=K_{ji}=A_c(i).G(j)=A_c(j).G(i)$.

3.4.2. Pre-Distribution for Mobile Devices

Firstly, mobile device starts communicate with MSP. The processing of key transferring from MSP is presented as follows:

1. $IP_M||Nonce_1||KEY\_REQ||MAC(K_{M2M},[IP_M||Nonce_1])$
2. $E(K_{M2M},[Nonce_1||S||ID_m])||MAC(K_{M2M},[Nonce_1||K_p||ID_m])$.

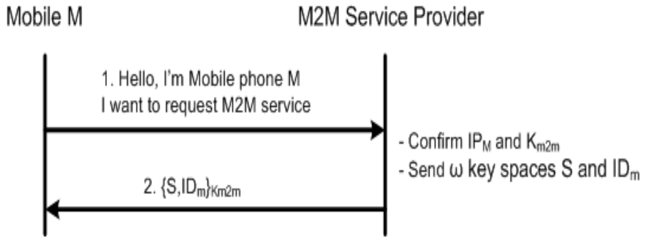

Mobile M
M2M Service Provider
1. Hello, I'm Mobile phone M
I want to request M2M service
- Confirm IP_M and K_{m2m}
- Send ω key spaces S and ID_m
2. $\{S,ID_m\}_{Km2m}$

Figure 5. Mobile device key pre-distribution.

An alternative is to use a M2M Service Provider (MSP) that stores keys of all mobile devices corresponding to their identities and key pool (K_p). In Figure 5, mobile M requests key for M2M service with package that includes the user's address (ID of mobile to communicate with MSP), M2M password (K_{M2M}), a random number (Nonce), a request message (KEY_REQ) for expected key and MAC. The MSP checks its database to see if the user has supplied the proper password for this user ID. If this condition is passed, the MSP accepts the user as authentic send *ω* key spaces (*S*) which include $\{A_1...A_\omega\}$ and *G(m)*; and identity ID_m (randomly choose identity in list M2M ID and concatenate with ID_{m2m} $([ID_{m2m} || ID_M]))$ to mobile device. This message is encrypted by K_{M2M} before sending. With *ω* key spaces, mobile device M has at least one common key space with any sensor node.

3.5. Authentication Phase

From this phase, mobile sink will use master key from key pre-distribution to authenticate with static sensor nodes. With derived key from MSP, user tries to authenticate with the closest neighbors in same domain as follows Figure 6.

Firstly, Mobile M tries to broadcast his identity ($ID_m= \{ID_{m2m} || ID_M\}$). When the static sensors receive ID_m, it is realized that this is M2M service ID because of prefix ID_{m2m} in ID_m. At that time, static sensors will send message with ID_m to gateway. Then gateway will ask MSP for legalization of ID_m. If ID_m is satisfied, gateway creates a new ID for mobile device (dynamic ID'_m) and send to static node which is the first static node sent request message to gateway. In this time, neighbor static node sends ID_b and one index of key space (S_c) to mobile M to create pairwise key. Then sensor and mobile M exchange seeds of *G(b)* and *G(m)*. At mobile M, S_c is existed in key space, then M tries to regenerate *G(b)* and calculate shared key $K_{mb}=A_c(m).G(b)$. After that, M sends a message with ID_m encrypted by key K_{mb} to node B. Node B also calculates and compares with this value $(K_{mb}=A_c(b).G(m))$. If two values are not equal $(K_{bm}\neq K_{mb})$, node B will reject all packages from this mobile M and remove ID'_m because there are attacker is faking ID_m. By contract, node B will send ID'_m encrypted by K_{bm}. When M receives packet, he decrypts and change ID by himself to ID'_m, calculate $K'_{mb}=F_{Kmb}$ (ID'_m, ID_b), where F_{Kmb} is one way hash function with key K_{mb}. Calculation shared key K'_{mb} is also occurred in node B similarly. So far, mobile and node B can communicate with shared key K'_{mb}. Node B will broadcast this new neighbor to his neighbor static nodes. Whenever M moves out of domain, gateway will broadcast this information to all static node in his domain to delete ID'_m.

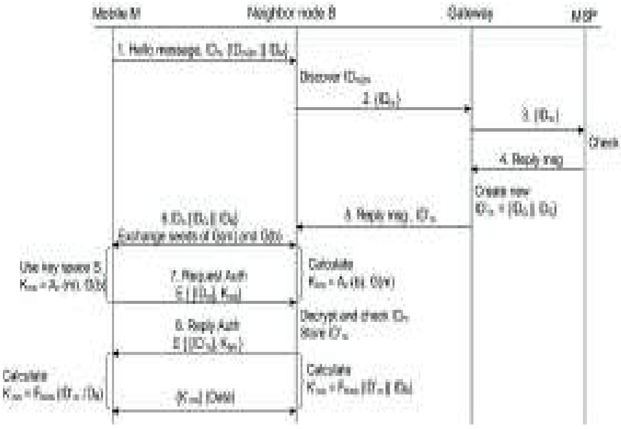


Figure 6. Mobile device authentication.

On the other hand, mobility is also considered in mobile sensors which are integrated in patient's body. Therefore, the below scheme helps mobile sensors can authenticate with static sensors in other domains.

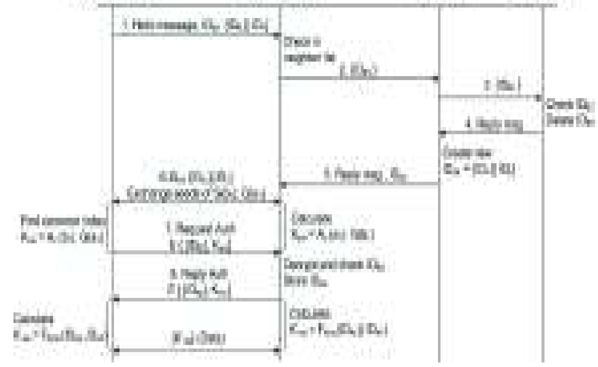


Figure 7. Mobile sensor authentication.

Mobile sensor authentication processing is almost same as mobile device (PDA) authentication. The discrepancy is mobile sensors is managed by gateways. Therefore, to check status of mobile sensors, gateway will base on ID_G (the prefix identity in each mobile sensor ID) to ask that gateway. In Figure 7, mobile sensor in domain B traverse to domain A. Gateway A will ask gateway B for his existence in domain B. Gateway B will monitor the status of mobile sensor B-1, it does not exist, gateway B will delete this ID_{B1} and broadcast to all neighbor in domain B. At this time, gateway A creates a new ID to admit this sensor nose as a new sensor node in domain A. After that, mobile sensor node will calculate K'_{ms} as shared key with his neighbor static node. Node A-1 will broadcast this new neighbor to his neighbor static nodes. If these two nodes can not find any common keys between them, they need to find a secure way to agree upon a common key. Therefore, the intermediary nodes are used to forward the message between the two terminal nodes.

- *Mobility:* In this mobility issue, there are two things which are considered: mobility of mobile phone and mobile sensor. Mobile phone is used by doctor who may traverse to the other domains has treatment to patients, mobile sensor is used by patients who may also be tested their health particularly in different rooms. Then, mobile phone or mobile sensor authenticates with static sensor node in that domain to resume gathering or transmitting data.
- *For Mobile Devices:* Armed with ω key spaces, doctor's devices can traverse any domain and always find at least one common key space with any sensor node, then establish a pairwise key to authenticate easily.
- *For Mobile Sensor:* Because of limited energy, mobile sensor can not keep key pool to calculate pairwise key. Therefore, whenever he moves out of domain, he has to send message in order to join the new domain. At that time, static sensor may check ID_d, if it is differ from his ID_d then a message will be sent to gateway to confirm. From gateway, it sends a message to mobile sensor's gateway to assure that whether mobile sensor does not exist in his domain. After checking existence of mobile sensor, mobile sensor's gateway broadcasts a message within domain to notice that ID of that sensor mobile ID_d left this domain. Then, mobile sensor uses new ID in the new domain to continue transmitting data.

Probability of sharing at least one key for mobile sensor, as above implementation, each domain has ω key spaces, and each sensor uses τ distinct key space to create common key. We use P_{SK} to represent the probability *(Pr)* of any two neighboring nodes sharing at least one space (i.e., they can find a common key between them). Since $P_{SK}=1-Pr$ (two nodes do not share any space) [12].

$$P_{SK} = 1 - \frac{\binom{\omega}{\tau}\binom{\omega-\tau}{\tau}}{\binom{\omega}{\tau}^2} = 1 - \frac{((\omega-\tau)!)^2}{(\omega-2\tau)!\tau!} \tag{1}$$

The values of P_{SK} have been plotted in Figure 8 when ω varies *m* to *100* and $\tau = 2,4,6,8$. For example, one can see that, when $\tau = 4$, the largest ω that we can chose while achieving the connectivity $P_{SK} \geq 0.5$ is *25*.

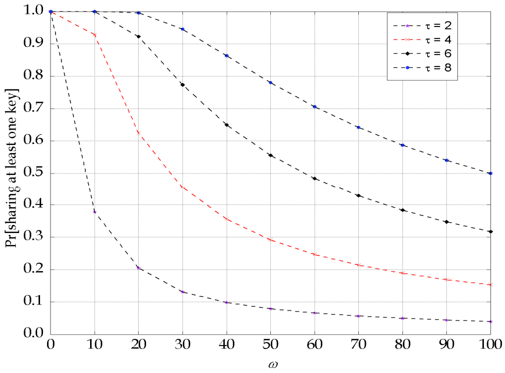


Figure 8. Probability of sharing at least one key when two nodes each randomly choose τ spaces from ω spaces.

4. Security Analysis

4.1. Probability of at Least one Space Being Broken

In general, the keys are not uniformly distributed among sensor nodes throughout the entire area, so the adversary may have a concentration in a local area to achieve a higher probability to compromise the nodes around a specified location. The adversary is assumed to know the key distribution mechanism that is deployed in the network. If the attacker finds that two nodes are in the signal range of each other, it means they may have a higher probability to share the common key spaces. The attack oriented key space of one domain: They attack to break the key space of one domain and then compromise the remaining nodes of other domains. Let S_i be the event that space S_i is broken, where $i=1 \ldots \omega$, ω is the number of the key spaces in the attack area and C_x is the event that *x* nodes are compromised in the attack area. According to the Union Bound, the probability that at least one space is broken is as follows:

$$\begin{aligned} &P(\text{at least one space is broken} \mid C_x = \\ &P(S1 \cup S2 \cup \ldots \cup S_\omega \mid C_x) \leq \sum_{i=1}^{\omega} P(S_i \mid C_x) \end{aligned} \tag{2}$$

where $S_i \cup S_j$ is the event that either space S_i or space S_j, or both, is broken. Because each domain is implemented same together, the probability of the broken key spaces, S_i and S_j, are equal. Therefore, equation 2 is changed to equation 3:

$$P(\textit{at least one space is broken}|C_x \le \sum_{i=1}^{\omega} P(S_i \setminus C_x) \le {}_{\omega} P(S_i \setminus C_x) \qquad (3)$$

Now we need to calculate *Pr* $(S_1|C_x)$, the probability of space S_1 being compromised when x nodes are compromised. Because each node carries information from m spaces, the probability that each compromised node carries information about S_1 is $\theta = \frac{\tau}{\omega}$. Therefore, after x node are compromised, the probability that exactly j of these x nodes contain information about S_1 is $C_x^j \theta^j (1-\theta)^{x-j}$, where θ is the probability that each compromised node carries information about S_1. Since space S_1 can only be broken after at least $\lambda+1$ nodes compromised, we have following result:

$$P(S_1|C_x) = \sum_{j=\lambda+1}^{x} \frac{x!}{j!(x-j)!} \theta^j (1-\theta)^{x-j} \qquad (4)$$

Combining equations 3 and 4, we have the following upper bound:

$$\begin{aligned} & P(\textit{at least one space is broken} \mid C_x) \le \omega P(S_1|C_x) \\ & \le \omega \sum_{j=\lambda+1}^{x} \frac{x!}{j!(x-j)!} \theta^j (1-\theta)^{x-j} \qquad (5) \\ & = \omega \sum_{j=\lambda+1}^{x} \frac{x!}{j!(x-j)!} (\frac{\tau}{\omega})^j (1-\frac{\tau}{\omega})^{x-j} \end{aligned}$$

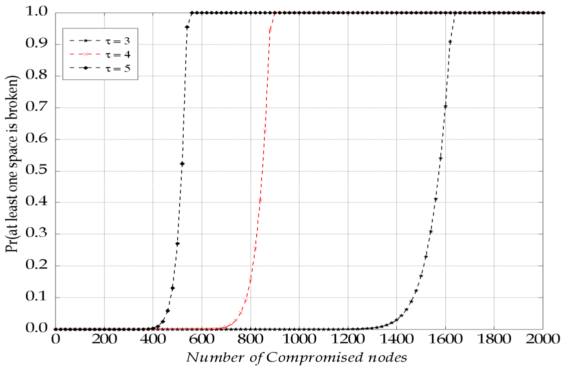


Figure 9. The probability of at least one key space being compromised by the adversary has captured x nodes (m=200, ω=100).

Figure 9 shows, for example, when the memory usage is set to *200*, *ω* is set *100*, and *τ* is set to *4*, the value of *λ* for each space is $49 = \left\lfloor \frac{200}{4} \right\rfloor - 1$, but an adversary needs to capture about 380 nodes in order to be able to break at least one key space with non-negligible probability.

4.2. Sybil Attacks

In [11] this type of attack is referred to Sybil attack. This attack on authentication process also can be applied easily to the replay attack like Distributed Denial of Service (DDoS) [17] on a sensor node or a gateway in wireless sensor networks.

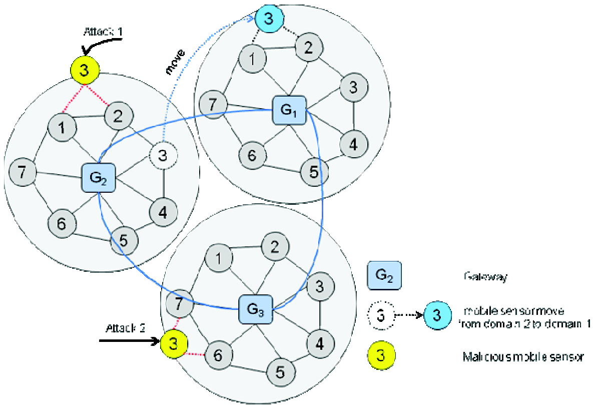


Figure 10. Sybil attack-mobile sensor.

Figure 10 shows a case of Sybil attack. In this case, mobile sensor 3 traverses from domain 2 to domain 1 and makes authentication with nodes in domain 1. Attacker 1 listens moving of mobile sensor 3, then he forges sensor 3 in domain 2 as the old mobile sensor which came back. Or the attacker 2 uses ID of mobile sensor 3 to try to communicate within domain 3. In the second case, base on communication between all gateways, gateway 3 will ask gateway 2 about sensor 3 and confirms that mobile sensor 3 moved out of domain 2, and then gateway 3 allows communicating with the forged sensor 3. Our proposed scheme can prevent this vulnerability by dynamic ID-based authentication. When mobile sensor moves to other domain, he will receive a new ID in new domain and the old ID will be erased in the old domain simultaneously. By this way, when attack 1 forges ID 3, ID 3 now does not exist in domain 2. For attack 2, gateway 3 has to ask gateway 1 instead of gateway 2, so attacker can not use ID 3 in domain because ID 3 is being domain 1.

6. Conclusions

In this paper, an M2M service has been introduced as an application in hospital. The proposed scheme is based on a dynamic ID-based authentication. Mobility of mobile devices and sensors are considered. The security analysis indicates that the proposed scheme provides a higher probability for non-compromised sensors to establish a secure communication in M2M service. Future works include validate our proposed scheme using simulation and real implementation.

Acknowledgement

This work was supported by the Korea Science and Engineering Foundation (KOSEF) grant funded by the Korea government (MEST) (No. 2010-0016959) and by the Ministry of Knowledge Economy (MKE), under Information Technology Research Center (ITRC) program supervised by the Institute of Information Technology Advancement (IITA) (NIPA-2010-

(C1090-1002-0002)). The corresponding author is Eui-Nam Huh.

References

[1] Blom R., "An Optimal Class of Symmetric Key Generation Systems," *in Proceedings of Advances in Cryptology, EUROCRYPT, Lecture Notes in Computer Science*, Berlin, pp. 335-338, 1985.

[2] Carman W., "New Directions in Sensor Network Key Management," *International Journal of Distributed Sensor Networks*, vol. 1, no. 1, pp. 3-15, 2005.

[3] Chan H. and Perrig A., "PIKE: Peer Intermediaries for Key Establishment in Sensor Networks," *in Proceedings of the IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies*, pp. 524-535, 2005.

[4] Chan H., Perrig A., and Song X., "Random key Predistribution Schemes for Sensor Networks," *in Proceedings of IEEE Symposium on Security and Privacy*, USA, pp. 197-213, 2003.

[5] Du W., Deng J., Han S., and Varshney K., "A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks," *in Proceedings of the 10th ACM Conference on Computer and Communications Security*, USA, pp. 77-82, 2003.

[6] Eschenauer L. and Gligor D., "A Key-Management Scheme for Distributed Sensor Networks," *in Proceedings of the 9th ACM Conference on Computer and Communications Security*, USA, pp. 41-47, 2002.

[7] Hegland M., Winjum E., Mjolsnes F., Rong C., Kure O., and Spilling P., "A Survey of Key Management in Ad-hoc Networks," *in IEEE Communications Surveys and Tutorials*, vol. 8, no. 3, pp. 48-66, 2006.

[8] Li G., He J., and Fu Y., "A Hexagon-Based Key Predistribution Scheme in Sensor Networks," *in Proceedings of the International Conference Workshops on Parallel Processing*, Columbus, pp. 175-180, 2006.

[9] Liu D. and Ning P., "Establishing Pairwise Keys in Distributed Sensor Networks," *in Proceedings of the 10th ACM Conference on Computer and Communications Security*, USA, pp. 52-61, 2003.

[10] Liu D. and Ning P., "Improving Key Predistribution with Deployment Knowledge in Static Sensor Networks," *ACM Transactions on Sensor Networks*, vol. 1, no. 2, pp. 204-239, 2005.

[11] Newsome J., Shi E., Song D., and Perrig A., "The Sybil Attack in Sensor Networks: Analysis and Defenses," *in Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks*, USA, pp. 259-268, 2004.

[12] Nguyen H., Guizani M., Minho J., and Huh N., "An Efficient Signal-Range-Based Probabilistic Key Predistribution Scheme in a Wireless Sensor Network," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 5, pp. 2482-2497, 2009.

[13] Perrig A., Szewczyk R., Wen V., Culler D., and Tygar J., "SPINS: Security Protocols for Sensor Networks," *in Proceedings of Wireless Networks*, USA, pp. 521-534, 2001.

[14] Rasheed A. and Mahapatra R., "An Efficient Key Distribution Scheme for Establishing Pairwise Keys with a Mobile Sink in Distributed Sensor Networks," *in Proceedings of the 27th IEEE International Performance, Computing and Communication*, Texas, pp. 264-270, 2008.

[15] Rasheed A. and Mahapatra R., "Mobile Sink Using Multiple Channels to Defend Against Wormhole Attacks in Wireless Sensor Networks," *in Proceedings of the 28th IEEE International Performance Computing and Communications Conference*, Scottsdale, AZ, pp. 216-222, 2009.

[16] Rivest R., "The MD5 Message-Digest Algorithm," *Technical Report*, MIT Laboratory for Computer Science and RSA Data Security, 1992.

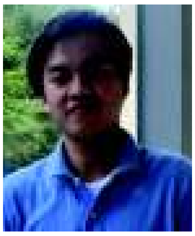
[17] Sachdeva M., Singh G., Kumar K., and Singh K., "DDoS Incidents and their Impact: a Review," *The International Arab Journal of Information Technology*, vol. 7, no. 1, pp. 14-21, 2010.

[18] Vaseashta A. and Vaseashta S., "A Survey of Sensor Network Security," *Sensors and Transducers Journal,* vol. 94, no. 7, pp. 91-102, 2007.

[19] Wang Y., Atterbury G., and Ramamurthy B., "A Survey of Security Issues in Wireless Sensor Networks," *IEEE Communications Surveys and Tutorials*, vol. 8, no. 2, pp. 2-23, 2006.

[20] Watro R., Kong D., Cuti S., Gardiner C., Lynn C., and Kruss P., "TinyPK: Securing Sensor Networks with Public Key Technology," *in Proceedings of the 2nd ACM Workshop on Security of Ad-hoc and Sensor Networks,* USA, pp. 59-64, 2004.

[21] Zhou L., Ni J., and Ravishankar V., "Efficient Key Establishment for Group-Based Wireless Sensor Deployments," *in Proceedings of the 4th ACM Workshop on Wireless security*, USA, pp. 1-10, 2005.



Tien-Dung Nguyen received his BSc degree in computer engineering from Ho Chi Minh University of Technology, Vietnam, in 2008. He is now an MS candidate in the Department of Computer Engineering, Kyung Hee University, South Korea. Under the guidance of Prof. Eui-Nam Huh, his interesting study areas are: key management, authentication, security protocols in wireless sensor networks, and cloud computing.

Eui-Nam Huh has earned BSc degree from Busan National University in Korea, MSc degree in computer science from the University of Texas, USA in 1995 and the PhD degree from the Ohio University, USA in 2002. He was a director of computer information center and assistant professor in Sahmyook University, South Korea during the academic year 2001 and 2002. He has also served for the WPDRTS/IPDPS community as program chair in 2003. He has been an editor of Journal of Korean Society for Internet Information and Korea Grid Standard group chair since 2002. He was also an assistant a professor in Seoul Women's University, South Korea. He is now with Kyung Hee University, South Korea as professor in the Department of Computer Engineering. His interesting research areas are: high performance network, sensor network, distributed real time system, grid, cloud computing, and network security.