Research Article

An Efficient Cluster Authentication Scheme Based on VANET Environment in M2M Application

You-Boo Jeon, 1 Keun-Ho Lee, 2 Doo-Soon Park, 3 and Chang-Sung Jeong 4

1 Visual Information Processing, Korea University, Seoul 136-713, Republic of Korea
2 Information and Communication, Baekseok University, Changcheongnam-do 330-704, Republic of Korea
3 Computer Software Engineering, SoonChunHyang University, Changcheongnam-do 336-745, Republic of Korea
4 Electronic and Computer Engineering, Korea University, Seoul 136-713, Republic of Korea

Correspondence should be addressed to Chang-Sung Jeong; csjeong@korea.ac.kr

Received 17 June 2013; Accepted 14 September 2013

Wireless and mobile sensor network technologies in M2M (machine to machine) are rapidly applied to our real life. Thus, in near future, advanced wireless and mobile sensor network in M2M application will be major key factor of the future generation convergence network which is based on the state of the application. It is expected that smart machines will appear as new business service model with other machines. Most numerous researches within M2M sectors are carried out in intelligent vehicle sector integrated with IT technology. Intelligent vehicle section shows severe changes in position between vehicles and has numerous large scales of networks in its components; therefore, it is required to provide safety by exchanging information between vehicles equipped with wireless communication function via VANET (vehicular ad hoc network) and fixed apparatus at roadside regarding the status of road. In this paper, we proposed cluster authentication scheme that mutually authenticates between vehicles by composing vehicle movement as cluster configuration architecture. We have successfully included the establishment of secure channels, the detection of replay attacks, mutual cluster authentication, prevention of vehicle identity fabrication, and secure distribution of provisional session key.

1. Introduction

Rapid development of IT has brought changes in development from personal PC to smart phone, and new service environment is constructed by converging with other peripheral devices based on smart phone. Now IT is leading rapid changes in society. The new field of “pervasive computing” has brought computing capabilities to the physical context and has expanded the intelligence of objects around us. Internet of things is the combination of the variety of information sensing machines and devices, such as radio frequency identification (RFID) devices, infrared sensors, global positioning system, and Internet, forming a huge network, so that all items are connected to the network to facilitate the identification and management, which ultimately provides the full range of services to people everywhere based on the integration of applications. The most important part in the network of things is the interconnection and interoperability between the machines, which is often called M2M. It is a general term of all that can enhance the communication of machinery equipment and capability of network technology, which organically combined in communication between machines, machine control communications, interactive communication, mobile internet communications, and other types of communication technologies, to share information with machine, equipment, application process, background information system, and operator [1].

Whenever and wherever information is obtained with no difficulty, and M2M, which is for communication between machines and surrounding devices, became a major research topic in technology among researchers and wireless communication entities. It creates new and various service environments by applying with new technologies. Research direction of M2M is to transmit a number of pieces of information via various communication environments between devices and machines. One of these researches is to integrate IT and
intelligent vehicles to enable various types of information to be transmitted, which means various devices are connected and linked to vehicles. Recent convergence technologies have impacted our life in various ways, and its technology is important to the extent that the country which initiates convergence technology is leading the world. IT technology is placed at the core of convergence, and the latter requires basis of IT. However, development of IT-based convergence technology bears a number of issues in itself, and the most critical factor is to ensure safety and security in communication between machines.

This research aims to examine what security factors exist in M2M and intelligent vehicles, then compose intelligent vehicles as cluster configuration architecture, and then propose authentication protocol of cluster unit. Finally, we show the performance evaluation of the proposed cluster authentication protocol.

2. Related Works

2.1. M2M Application Service and Security. M2M service is defined as machine to machine, machine to man, and man to machine. As depicted in Figure 1, various devices are installed to communicate and collect information from surrounding equipment and devices. Its concept is to provide information service to people and surrounding machines. M2M is utilized in the sectors of sensor network, tracking, c, and emerging device. Core technologies in M2M are identification, information collection, communication, intelligence, and minimization, and every device and system should be maintained autonomously and securely through control and information exchange between machines [2].

Threatening factors in devices in M2M architecture are bugging between equipment, hijacking, and alteration of privacy in relation with denial. There are possible threatening factors in gateway such as authorization violation by illegal usage and access, physical intrusion, replay attack, and man-in-the-middle attack. Other types of threatening factors are paralysis through illegal intrusion, service denial, virus, worm, troy wooden horse, and depletion of resources [2].

2.2. Intelligent Vehicle Security Requirements. Wireless ad hoc networks are currently a very active area of academic and industrial research for their foreseeable broad applications. These networks do not have any fixed infrastructure. The vehicles in ad hoc networks are usually limited devices with respect to their energy sources, computational capabilities, and communication range. However, it is vulnerable to a wide range of attacks due to the open medium, dynamically changing topology, possible vehicle compromise, difficulty in physical protection, absence of infrastructure, and lack of trust among vehicles [3]. Policing traffic management (PTM) is applied to improve the quality of service (QoS) over an intervehicular communications system (IVCS) [4]. The security threats have been extensively discussed and investigated in the wired and wireless networks; the correspondingly perplexing situation has also happened in MANET due to the inherent design defects. There are many security issues which have been studied in recent years. For instance, snooping attacks, wormhole attacks, black hole attacks, routing table overflow and poisoning attacks, packet replication, denial of service (DoS) attacks, and distributed DoS (DDoS) attacks. Specially, the misbehavior routing problem is one of the popularized security threats such as black hole attacks. Some researchers propose their secure routing idea to solve this issue, but the security problem is still unable to prevent completely [5].

Intelligent vehicle is evolving with various types of services to provide convenience of life by integrating with home network, telematics, and intelligent robot, thanks to development of convergence technology. Service models of intelligent vehicle are car to enterprise (C2E), car to car...
(C2C), and car to home (C2H). As seen in Figure 2, intelligent vehicle communication network technology is classified with internal network and external network of vehicle from the reference point of vehicle as illustrated in Figure 3. Internal network of vehicle is in general called IVN, whereas external network of vehicle is divided into V2V (vehicle to vehicle) and V2I (vehicle to infrastructure). IVN is composed of CAN, which connects and controls body or frame of car, MOST, which is for access to multimedia devices such as audio, amp, and CDP of vehicle, and X-by-Wire which connects and controls break or steering. V2V establishes vehicle communication network which constructs communication network based on vehicle-to-vehicle communication without having infrastructure of transmitting information, whereas V2I lets the vehicle access infranetwork via wire and wireless communication and provides communication network that supports communication between terminals and servers. V2V provides vehicle collision warning services and group communication based on communication between vehicles, whereas V2I provides IP based traffic information and safety support and downloads service to vehicles [6–8].

Intelligent transmission system (ITS) is an intelligent traffic system applied with state-of-the-art scientific technologies such as computer, communication, and electronics for improving existing traffic system more efficiently and economically in terms of solving traffic delay, accident, and
air pollution. ITS is composed of various types of information transmission systems such as ATMS (Advanced Traffic Management System), ATIS (Advanced Traveler Information System), APTS (Advanced Public Transportation System), CVO (Commercial Vehicle Operation), and AVHS (Advanced Vehicle and Highway System).

However, there are some dysfunctions of intelligent vehicle services: violation of personal information and privacy, vehicle information, communication messages between vehicles, and communication traffic information. It requires safe and secure message transmission against these threats and forgery. There are some security framework of intelligent vehicle for the safe and secure vehicle services and communications: secure positioning, vehicle-to-infrastructure secure communication, vehicle-to-vehicle secure communication and user access control, and VPKI (Vehicles PKI).

Security treat factors in intelligent vehicle lie in network aspects. One type of security treat is forgery in which one vehicle generates false information and transmits to other vehicles located in a certain network zone. The other treat is jamming attack which generates interfering signal to other vehicles located in a certain network zone. Information forgery is executed with drop, corrupt, or modified messages or information in the process of transmission in the running of vehicle. Impersonation attack is executed in a way of in-transit traffic tampering and modifying of vehicle status information for misleading other cars. Privacy violation is executed in a way of infringement of personal privacy related information such as time, location, vehicle ID, and movement information of vehicle. On-board tampering is executed in a way of modifying speed, position, vehicle interior status information, and various sensing information of on-board vehicle [6, 9].

We present the security requirements for our VANET security system and will show the fulfillment of these requirements after presenting the design details. The privacy requirements state that private information such as vehicle owner’s identity and location privacy is preserved against unlawful tracing and user profiling. A secure VANET system should satisfy several fundamental requirements, namely, authentication, nonrepudiation, message integrity, and confidentiality, where sensitive information is being exchanged, to protect the system against unauthorized-message injection, denial of message disseminations, message alteration, and eavesdropping, respectively. Nonrepudiation also requires that violators or misbehaving users cannot deny the fact that they have violated the law or misbehaved [10].

3. Cluster Configuration Scheme

This scheme uses the same two types of messages used in the CH(v) and Join(v, u). This CH (ClusterHead) selection scheme uses Cluster(v) and ClusterHead to indicate the set of vehicles in the cluster whose CH is v and the CH of a vehicle’s cluster, respectively. CH(v), the Boolean variable of v, is set to true if v has sent a CH message. Its variables ClusterHead, CH(–), and Cluster(–) are initialized to nil, false, and zero, respectively.

The cluster topology is initialized and maintained through the periodic transmission of messages by each vehicle. When a vehicle is initialized, it has an undefined status cluster. To set its status cluster, it must determine whether it is within the bounds of any currently defined clusters. The vehicle broadcasts a message to its neighbors to announce its presence and to search for a neighboring CH. In the event that all vehicles initialize simultaneously, the vehicles broadcast messages looking for neighboring CHs at approximately the same time.

The following describes the two procedures that are executed at each vehicle v. On receiving a CH message from neighbor u, vehicle v checks to see whether it has received messages from all its neighbors z and that w_u > w_z, as indicated by a Join(z, v) message. In this case, v will not receive a CH message from these neighboring vehicles. Therefore, by default, u is the vehicle with the greatest weight in v’s neighborhood that has sent a CH message. At the initial clustering setup or when vehicle v is added to the network, vehicle v executes the CH-selection procedure in order to determine its own role. If its neighbors include at least one CH with a greater weight, then v will join it. Otherwise, it will be a CH [II].

Note that a neighbor with a greater weight that has not yet decided its role will eventually send a message. If this message is a CH message, then vehicle v will try to affiliate with the new CH. When vehicle v receives the corresponding CH message, it checks to see if w_u > w_v. If this is the case, then v joins n’s cluster independent of its current role [II]. When a neighbor u becomes a CH, on receiving the corresponding CH message, vehicle v checks whether it has to affiliate with u; that is, it checks whether w_u is greater than the weight of v’s CH. In this case, independent of its current role, v joins u’s cluster.

Every vehicle must either be a member of a cluster or else be a CH. Hence, if a vehicle is not within the transmission range of any CH, it should be a CH itself. When a vehicle moves to the periphery of a network, it is possible that it will move out of direct transmission range of all other CHs. When a vehicle loses contact with all CHs, it transmits a message to look for another CH, to verify that it is not within the transmission range of any CH. It then sets a timer to wait for the reception of a message from a CH. As vehicle s wander to the periphery of a network, it is likely that they will become CHs because they will be out of transmission range of all other CHs. To prevent continued growth in the number of CHs, there must be a mechanism for CHs to revoke their CH status and become non-CHs. A number of clustering protocols have the requirement that when two CHs come within direct transmission range of one another, one CH must give up its CH status. The protocol for deciding which CH should revoke its CH status can be based on a weighted algorithm. This results in a ripple effect, whereby one CH change results in additional changes within the network. CH changes are expensive due to the change in routing paths that occur as a result. Therefore, the ripple effect can have a detrimental impact on the performance of a network and should be avoided. Hence, CH changes should be minimized. This algorithm minimizes CH changes during


4. Cluster Based Authentication Protocol

4.1. Assumption. Protocol environment is proposed based on the following hypotheses: all vehicles are running in the same environment. Each vehicle is represented as a vehicle in Figure 4 with weighted reference on the basis of structure of Figure 2. First, vehicle in running is authorized from server via RSU. DoS (denial of service) attack is possible in physical layers of real network. But this DoS attack is not considered. Second, in the cluster configuration, each vehicle is supposed to know vehicle information received from RSU or surrounding vehicles. RSU ensures safe connection in communication between authorizing server and CH (ClusterHead). CH maintains ID$_i$ of vehicles within cluster, and each CH should be always reliable. CH is assumed to play a role as a server within cluster. Each vehicle is randomly composed with weighted value for each vehicle as seen in Figure 4 according to selection criteria of CH.

It is assumed that references of weighted value are determined on the basis of characteristics of vehicle (speed, distance of vehicles, and calculation function of vehicle). When authorization of vehicles is expired, it will be disposed immediately and receives a new one. Authorization via CH is reissued by using key of each vehicle from authentication server.

Each cluster is composed as Cluster A, B, and C on the basis of Figure 4. Relationship with neighbor vehicles and weighted value are the criteria in cluster composition. CH in Cluster A, vehicle 2 shows highest weighted value 7, so it plays as a ClusterHead. It is assumed that vehicle 3 in Cluster B and vehicle 5 in Cluster C play a CH role, respectively. The vehicle approaching in cluster plays gateway for connecting each cluster.

4.2. Symbols. The following symbols are used in this research.

- CH$_A$: ClusterHead A
- ID$_X$: Identification X
- K$_{S,CH}$: Confidential key shared between session key S and CH or S and CH
- Time: Current time
- S: CH$_A$ member vehicle
- X: CH$_B$ member vehicle
- K$_{A+}$: Public key of vehicle A
- K$_{A-}$: Private key of vehicle A
- cert$_A$: Certification of vehicle A
- $e$: Effective date of authentication
- Nonce$_A$: Vehicle A nonce generation.
4.3. Authentication Scheme and Protocol. Cluster authentication protocol is composed of authentication protocol with cluster units without existing infrastructure and one with existing infrastructure.

4.3.1. Noninfrastructure Authentication Scheme. Noninfrastructure authentication method is to authorize with signature between ClusterHeads as depicted in Figure 5. It provides security between clusters by using session key as a key value.

After authenticating a CH using the server, there are nine steps in our end-to-end key exchange procedure and authentication process for Noninfrastructure networks, as shown in Figure 5. First, using a previously shared secret key $K_{S,CH_A}$, $S$ sends a message to $CH_A$ requesting communication with $X$. Since $ID_S$ is encrypted using $K_{S,CH_A}$, only vehicles $S$ and $CH_A$ know the vehicle with which $S$ wishes to communicate. As $Cert_S$ and $Nonce_S$ are also encrypted, they can be transferred securely.

On receiving the request, $CH_A$ checks to see whether $S$ is a member. If this is the case, steps 2 and 6 shown in Figure 6 are not required. Otherwise, in step 2, $CH_A$ asks the other ClusterHeads where $X$ is using their public keys. Let us assume that $X$ is located in cluster $B$. By using the $CH_B$ public key that was previously established for communication between CHs, the search reveals that $X$ is located in cluster $B$.

In step 3, $X$ is informed of the request from $S$ to communicate with it. $CH_B$ sends $S$'s certificate along with $Nonce_{CH_B}$. On deriving the public key for $S$ from the certificate, $X$ calculates the session key $K_{X,S} = (PK_X)^K_S \mod P$ using $PK_X$ derived from $Cert_X$. Finally, in step 9, $S$ communicates with $X$ by sending back $X$'s nonce encrypted using their shared key $K_{S,X}$.

4.3.2. Changing Vehicle into Cluster. A vehicle joining a cluster for the first time needs strong authentication. We use the system key pair because it allows mutual authentication between the joining vehicle and an existing member vehicle of the cluster. When a vehicle joins a cluster, it is given a system public key and a system private key. All the vehicles of the cluster share this key pair. When a new vehicle moves into the network and is detected by the $CH$, it is given the cluster key and the table containing the cluster IDs, shadow key (SK), and $CH$ public keys. The $CH$ acts as the certification authority for all of its members. This information is exchanged after mutual authentication in which the corresponding CHs of the vehicles act as servers. The $CH$ keys are used to exchange session keys secretly. The $CH$ then decrypts and transmits the session key to other members involved in the session. If a vehicle wants to establish a session with other vehicles, it also sends this request to the $CH$. The $CH$ generates a set of random prime numbers. First, the numbers are encrypted with the $CH$'s private key and then with the cluster key. Along with each number, a timestamp is encrypted so that the keys can be used for only a limited amount of time. All the other cluster members also receive this information and buffer the values, since these number values can serve as authentication.

As the composition of a CH network changes dynamically when CHs are added, deleted, or merged in the network, the secret shares must also be renewed regularly because the number of shares needs to adapt to the number of CHs. In addition, it is necessary to ensure that the key shares are renewed after a certain period of time to make it difficult for a moving attacker to compromise several SK CHs over time.
In our approach, we always combine the addition, deletion, and merging of CHs with key share renewal and only schedule additional renewals if the CH network remains unchanged for some time. The public key of the CH network must be known to all vehicles in the VANET. It is propagated via the CH beacons, which are broadcast periodically in every cluster. Besides the public network key, a CH beacon also contains the CH’s own public key, a list of vehicles in the current cluster, including their status, and a list of gateways connected to adjacent clusters. This beacon message contains information regarding the neighbors, including the clusters that they belong to, adjacent clusters, and certificates. On receiving a message, a vehicle updates its local related tables with the message information and can detect vehicles that are joining or leaving. This method provides a useful means of maintaining cluster membership synchronization.

Figure 6 shows the join situation. When a vehicle joins a cluster area for the first time, the CH detects that a new vehicle has joined based on the messages in Figure 6(b). When a vehicle leaves a cluster or joins a new cluster area, the system begins the CH selection algorithm for remaining vehiclesthathavenotyetbeenchosenasCHsorgethemselvesasstatedinFigure 6(a). The CH at the old location receives newer messages from its one- and two-hop neighbors that do not contain the member entities of the leaving vehicle for a predefined time interval, at which point the old CH purges the leaving vehicle.

When a new vehicle joins the network and is detected by a CH, it receives the cluster key and the table containing the cluster IDs, lifetime, mobility, weight, and CH public keys. When a vehicle leaves a cluster and joins another cluster with the movement of vehicles, the new CH treats it as a new vehicle joining its cluster. Mutual authentication is performed between the moved vehicle and its new CH using the system key pair (K/k). The CH then gives the vehicle the cluster key for the new cluster. The old cluster purges the entry for this vehicle when it does not receive a message within a predefined time interval.

The merging of two clusters into a single cluster is one of the most difficult and expensive operations. As two cluster SKs cannot be mixed, one must be dropped and the other distributed over the entire network. All of the certificates that were signed with the dropped key eventually have to be reissued, although it is possible to keep the dropped key for a period of time to facilitate this process. It may become necessary to adapt a (K, SK) threshold for the changed number of vehicles and CHs in the networks. If merging two bigger networks is difficult, any decision about the remaining network depends on parameters such as the number of CHs and the number of vehicles that would like to apply for a new configuration cluster using the CH selection algorithm and obtain new certificates.

### 4.3.3. Infrastructure Authentication

Figure 7 shows authentication protocol between terminals on the basis of Figure 4 cluster composition. In order to authorize via other RSU, it needs to receive authentication by using server key from authentication server and confirm whether CH is registered in authentication server. In the fast moving environment of intelligence vehicle where its status keeps changing, the changes of each vehicle...
can be checked by cluster unit. This brings efficiency of management. In the event that vehicle 1 in Figure 4 moves quickly to Cluster B zone at other RSU zone, CHB, for proceeding of authentication work for this vehicle, can check whether this is the right vehicle by communication with CHB which used to maintain vehicle 1 from authentication server.

Where, the server is reliable and officially certified server and maintains CH through each RSU. This is able to react to malicious attack against each vehicle by transmitting to server information about newly approaching vehicle to RSU and leaving vehicle on a real time basis. Every CH can initiate authentication work by receiving authentication from reliable server. As seen in Figure 4, in the event that CH misses message of vehicle, it can transmit correct message by threshold. Security is ensured by that CH knows public key of server and private key of each CH.

Upon request for communication between each CH, ID of CH, current time, and Nonce are generated and sent, and server transmits authentication including effective date. This is how mutual authentication is made between CHs.

5. Attack Analysis

In this section, we compare the efficiency of existing clustering protocols and our proposed protocol. We also discuss how authentication scheme and protocol is able to deny possible attacks in VANET. As scheme and protocol establishes authentication based on a trusted layer, it guarantees end-to-end security.

We evaluated the performance of our protocol and identified the advantages and limitations of our proposed approach. In our protocol, a CH establishes a member vehicle that is worthy of trust by the other members of the CH. Falsehood detection in the certification process is achieved. Authentication scheme and protocol is more reliable during the certification of a CH because it uses a server and it has fewer processing operations. The scheme and protocol enforces stronger security as it uses a server to obtain a higher level of security than can be realized by other clustering routing protocols.

An analysis of its performance verified its authentication, efficiency, safety, and scalability. Authentication and nonrepudiation use a cryptographic certificate. Each vehicle receives a certificate from its trusted CH. We evaluated four performance metrics.

5.1. Modification Attacks. Attacks using modification are generally targeted against the integrity of routing computations. By modifying routing information, an attacker can cause network traffic to be dropped, redirected to a different destination, or take a longer route to its destination, resulting in increased communication delays.

Proposed scheme and protocol can use the session keys to encrypt the traffic flow of both data and control packets. Therefore, since the Diffie-Hellman key exchange \( K_{XS} = (PK_S)^{Xs} \mod P \) of the message contents is included in every packet transmitted, the integrity of the contents is guaranteed, along with confidentiality.

5.2. Fabrication Attack. Fabrication attacks involve generating false routing messages. These attacks are difficult to recognize as they are received as genuine routing packets. An attacker can nullify a working route to a destination by fabricating a routing error message claiming that a neighbor can no longer be contacted.

The authenticity of the received control and data packets can be verified using the session keys and the server. As the session keys are unique, fabricated packets can easily be detected and hence discarded.

5.3. Spoofed Route Attack and Unauthorized Participation. A malicious vehicle can launch several attacks in a network by masquerading as another vehicle (spoofing). Spoofing occurs when a malicious vehicle misrepresents its identity by altering its MAC or IP address in order to fool a benign vehicle into arriving at an inaccurate picture of the network topology.

Proposed scheme and protocol participation accepts only packets that have been signed with a certified key issued by a trusted authority using a server. There are many mechanisms for authenticating users to a trusted certificate authority. Since only the source vehicle can sign using its own private key, vehicles cannot spoof other vehicles in route instantiation. The encryption of all end-to-end traffic indirectly ensures the verification of packets, as the session keys are held only by the previously authenticated end points. Consequently, the legitimacy of all packets is verified automatically during the decryption phase, ensuring that any packets that were spoofed are discarded. Similarly, replay packets include the destination vehicle’s certificate and signature, ensuring that only the destination can respond to route discovery.

5.4. Replay Attacks. When the attacker receives a request for a route to the target vehicle, the attacker creates a replay in which an extremely short route is advertised. If the malicious replay reaches the requesting vehicle before the replay from the actual vehicle, a forged route has been created.

Replay attacks are prevented by including a nonce and a timestamp with the routing message. Proposed scheme and protocol minimizes changes in the certificate process of cluster networks. Our analysis of scalability has verified the authentication, efficiency, safety, and scalability of our method.

6. Conclusion

It is expected that various security issues are raised in the development of intelligent vehicle and its convergence technology. Future security issues in vehicle industry have inherently critical treat factors; therefore, it is important to research on security. Among all other security threatening factors, this research has proposed authentication protocol on a cluster basis to counteract various changes in vehicle. Proposed protocol can improve safety and security by effective authentication in a scalable wide area such as express road environment. For the future further research subjects in cluster configuration, it may require to research about an algorithm which can configure more efficiently with various
changes and increase security level while reducing resources in the middle of various changes.

Acknowledgments

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 (no. 2011-0010457). This research was supported by the MKE (Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program supervised by the NIPA (National IT Industry Promotion Agency) (NIPA-2012-C1090-1201-0008).

References

[1] J. Du and S. Chao, "A study of information security for M2M of IOT," in Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE '10), pp. V3576–V3579, August 2010.
[2] G.-S. Ryu and K.-H. Lee, "Authentication based on cluster in machine to machine," Journal of the Korea Knowledge Information Technology Society, vol. 5, no. 6, pp. 103–110, 2010.
[3] M. Imani, M. Taheri, and M. Naderi, "Security enhanced routing protocol for Ad hoc networks," Journal of Convergence, vol. 1, no. 1, pp. 43–48, 2010.
[4] S. Prahmkaew, "Performance evaluation of convergence Ad hoc networks," Journal of Convergence, vol. 1, no. 1, pp. 101–106, 2010.
[5] F.-H. Tseng, L.-D. Chou, and H.-C. Chao, "A survey of black hole attacks in wireless mobile Ad hoc networks," Human-Centric Computing and Information Sciences, vol. 1, article 4, 2011.
[6] G.-W. Kim, S.-K. Kim, and K.-H. Lee, "The security requirement based on intelligent vehicular network in M2M environment," Journal of the Korea Knowledge Information Technology Society, vol. 5, no. 6, pp. 124–129, 2010.
[7] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," IEEE Wireless Communications, vol. 13, no. 5, pp. 8–15, 2006.
[8] I. Cha, Y. Shah, A. U. Schmidt, A. Leicher, M. Victor, and Trust in M2M communication, IEEE Vehicular Technology Magazine, vol. 4, no. 3, pp. 69–75, 2009.
[9] D.-R. Kim, J.-Y. Song, and S.-K. Cha, "Introduction of case study for M2M intelligent machine tools," in Proceedings of the IEEE International Symposium on Assembly and Manufacturing (ISAM ’09), pp. 408–411, November 2009.
[10] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular Ad hoc networks," IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 9, pp. 1227–1239, 2010.
[11] S. Basagni, "Distributed clustering for Ad hoc networks," in Proceedings of the 1999 International Symposium on Parallel Architectures, Algorithms, and Networks (ISPAN ’99), pp. 310–315, June 1999.
Submit your manuscripts at http://www.hindawi.com