An Identification based Authentication Protocol for Secure Data Transmission in Ad-Hoc Networks

Youngbok Cho, Sun Ning and Sangho Lee*

Network Security Lab, Chungbuk National University,
410 Seongbong-ro, Heungdeok-gu,
Cheongju, Republic of Korea
**Dept.of Softerwer, Electrical Information,*
Chungbuk National University,
410 Seongbong-ro, Heungdeok-gu,
Cheongju, Republic of Korea
{bogicho, sunn2001, shlee@cbnu.ac.kr}

Abstract

Wireless ad hoc network is most important present minimizing energy consumption. Among various clustering methods, the low-energy adaptive clustering hierarchy (LEACH) mechanism takes the hierarchical approach of segmenting multiple clusters for efficient energy management. The mechanism, however, configures new clusters in every round, so the energy consumed whenever configuring clusters shortens the useful lifetime of the entire network. For this reason, this paper generates clusters and selects candidate cluster head (CCH) in the initial round under the ad-hoc network environment. Subsequent rounds continue, without performing re-clustering, until all of the candidate cluster heads selected become cluster head (CH), thereby addressing the issue of energy consumption in the setup phase for clustering. The proposed model consumes around 30% more energy than the conventional LEACH in the initial round, but its total energy consumption declines in as the round continues. The network simulation tool (NS-2) proves that its energy efficiency improves by up to 13.3% in the 1,000-node environment compared to when 100 sink nodes are employed.

Keywords: *Ad-hoc Network, Clustering, Hierarchical, LEACH, Energy Efficient, Sink Node*

1. Introduction

Wireless ad-hoc networks widely applications in real-time traffic monitoring, military data collection, earthquake analysis and measurement of environment pollution etc. Wireless ad-hoc networks consist of very tiny sink nodes which usually have the limitation such as memory size, calculation capability, and radius of communication. Sink nodes are always exposed in hostile environment and wireless communication are easily tapped by others. Furthermore, messages could be modified and replied by the attackers, so, secure wireless communications should be an important issue in wireless ad-hoc networks. Consequently, much various methods in secure wireless ad-hoc network have been researched. Due to the limitations of sink node and characteristic of wireless communication, routing attacks such as capture, destroy, listening (tapped), DoS, sink hole and worm hole are very weak in ad-hoc networks. Consequently, to implement the secure demeans of message integrity,

confidentialness and nodes authentication, researches on light key distribution and authentication mechanism for wireless networks are popular.

To suit of sink node, Ref [2, 11] proposed method to lighten the existing public key mechanism which needs much calculation, In μ -TESLA [5] of SPINs and LEAP [7], secure key distribution methods with low computing capability are proposed. Also, private key method was proposed in PIKE [8] and if the private key is expose, key pre-distribution method was proposed in Ref [6]. Also, IDE mechanisms are proposed in Ref [9, 10, 11, 12], in which, it's not necessary to use key distribution and number of messages is reduced. Due to the wireless communication, message is easily be listened by attackers. To avoid this, it's necessary to encrypt the transmitted data between nodes.

In Ref [12], data encryption mechanism AM-E is proposed, in AM-E, when base station generates authentication key, it uses ID and residual energy of sink node. To generate authentication key, all sink nodes can directly communication with base station. But in reality, it's difficult for all nodes to directly communicate with base station. To directly communicate with base station faraway, nodes with limited energy need send authentication messages firstly. This increases the energy consumption. So nodes which consumed much energy can't transmit data for a long time. Therefore, in order to securely transmit data in ad-hoc networks, an IDE-based hierarchical node authentication proposed in our proposed in our paper.

This paper solved the problem that too much energy is consumed during the generation of authentication key because sink nodes directly communicate with base station in Ref [12]. This proposed paper uses logical hierarchical structure for nodes authentication. All nodes are divided with logical clustering structure. After authentication, base station distribution session key to cluster head, then each sink node receives the group key through cluster head.

Compared with the existing symmetric key and ID-based mechanisms, number of messages to authenticate is minimized and secure communication is assured through authentication of nodes in this paper. By using group key and session key mechanisms, the experiment result showed that the energy consumption in first round is reduced about 34% and the total energy consumption with 1000 joined nodes in the entre lifetime is reduced about 29% compared with Ref [12].

The remaining part of this paper is organized as follows: In Section 2 discuss the related works including distance based energy consumption model for wireless communication and ID-based authentication frame work for ad-hoc network. Session 3 introduce our IDE-based hierarchical protocol for node authentication to securely transmit data in ad-hoc network. Session 4 states the simulation environment and results for our proposed protocol. Finally, Session 5 draws the conclusion.

2. Related Works

2.1 Energy Consumption of Wireless Communication

In wireless communication, energy consumption is increased with the distance increasing. For example, transmission of k-bits message to a certain distance needs energy as (equation 1).

$$E_{tk}(k,d) = \begin{cases} k \times E_{elec} + k \times e_{fs} \times d^2, d < d_0 \\ k \times E_{elec} + k \times e_{fs} \times d^4, d \geq d_0 \end{cases} \quad (1)$$

$$E_{rx}(k) = k \times E_{elec}$$

We use a simplified model shown in Heinzelman et al. (2002) for the radio hardware energy dissipation as the above. To transmit an k-bit data to a distance d, the energy consumes in transmission and receive. In equation (1), E_{tx} is the energy consumption in data transmission and E_{tx} is the energy consumption in data receiving. ε_{fs} means the amplifier energy, whereas E_{elec} means the electronics energy. $\varepsilon_{fs} \times d^2$ or $\varepsilon_{amp} \times d^4$ depends on the distance to the receiver.

Account for the limitation of sink node, it's necessary to reduce the energy consumption during the data transmission. Since direct transmission between sink node and base station is not efficient in energy consumption, hierarchical structure for data transmission is proposed.

2.2 Existing Mechanisms for Ad-hoc Networks

The key management mechanisms for ad-hoc networks have been researched in various ways. Before nodes deployment, according to whether master key should be used, key distribution mechanisms classified into three types: pre-distribution mechanism [3], mechanism based on master key [7] and mechanism based on base station [10]. In Ref [3], in order to assure the authentication between nodes, a secure mechanism consists of three steps. In probability scheme, the problem that not all nodes can connect with each other arises. Furthermore, in the situations where nodes are irregularly deployed or there is communication interruption, the problem gets more serious. In LEAP [7], there are four cryptographic keys, including private key, group key, cluster key and pair-wise key. In the above keys, private key and group key is installed in sink node before deployment, so attacker can capture sink nodes to get the key information. In HIKES [10], base station acts as the Trust Authority (TA) and authorizes parts of the function to cluster head. All nodes generate authentication key using partial key escrow and elect the cluster head. After data aggregation, cluster head transmits the aggregated data to base station. Since node needs authenticate with base station, parts of nodes may consume much energy for a very far distance to base station. Whereas the save memory for practical key escrow table may expire too. Attacker can get the partial key escrow table by node capture and with it cause inference to cluster head and pair-wise key of nodes in other place. In the same time, with the increasing of sink nodes in the cluster, more energy consumption is needs for authentication between cluster head and nodes. This results in the decreasing of network lifetime.

2.3 IDE based Authentication Framework for Ad-hoc Network

The ID-based-encryption (IBE) framework was firstly proposed by Shamir [9] and has got various developments since then. IBE mechanism is suitable for ad-hoc network because pre-distribution of keys is not necessary and low computing capability is only needed. IBE has the same secure level as RSA and is characterized by short computing time and low memory necessity.

In Ref [12], ID based 2-mode authentication framework consists of pre-communication phase and communication phase. In pre-communication phase, after being deployed nodes set up the neighbor node table and find the routing path by sending Hello message, then search cluster head according to the neighbor table and routing path before communication.

Pre-communication phase consists of four steps as flows:

Step1. The sink node announces themselves with other neighbor nodes through using hello message and their ID.

Step2. The neighbor nodes exchange the IDs to discover if they share the common keys.

Step3. If the common keys exist, these IDs are kept at the node as the trust allies and a path in the communication graph is established.

Step4. Basing on the graph, the routing algorithms are used to find the routine to the cluster head. This routing information is updated at each nodes routing table.

In communication phase, there are two types of communications: communication after node authentication and communication without node authentication. Communication message is encrypted using K_e which is generated by MAC mechanism before communication. K_a, K_e is generated by using one way hash function of F. The keys are pre-distributed. In node authentication phase, it's realized by comparing the neighbor table of nodes and member node table of cluster head. In 2–mode authentication framework, sink nodes exchange the ID and pre-distribution key and compare with the trusted neighbor table. If it's match, they authenticate each other. When a node receives an authentication request (AREQ) message. Because only ID is included in the message, the receiver can't verify if the source is legal. So the authentication mechanism where ID includes the source information and verification of source can be confirmed is necessary.

When cluster head is changing, attacker send cluster head advertisement message to nodes in the cluster. This could be a deadly threat to nodes in the cluster. Furthermore if the security mechanism if applied, number of AREQ message is large results in the oversupply energy consumption problem.

3 IDE-based Hierarchical Node Authentication Protocol

In this section, IDE-based hierarchical node authentication mechanism for secure transmission of data is proposed. In existing IDE-based papers, source verification through AREQ message and node authentication through direct communication between nodes and base station cause serious energy consumption. This paper aims to solve the above problem. In the view of security, this paper also proposed a mechanism which strengthens the security of node authentication message reply and realizes the secure data collection.

3.1. Overview of Proposed Model

In this paper, we proposed an IDE-based an IDE-based hierarchical node authentication model. Base station serves as the CA of first level to authenticate all cluster heads. If the

cluster head is authenticated by base station, in order to authenticate the member nodes within its cluster, the cluster head serves as the second level CA and generates the key applied for member nodes to communicate with the CA.

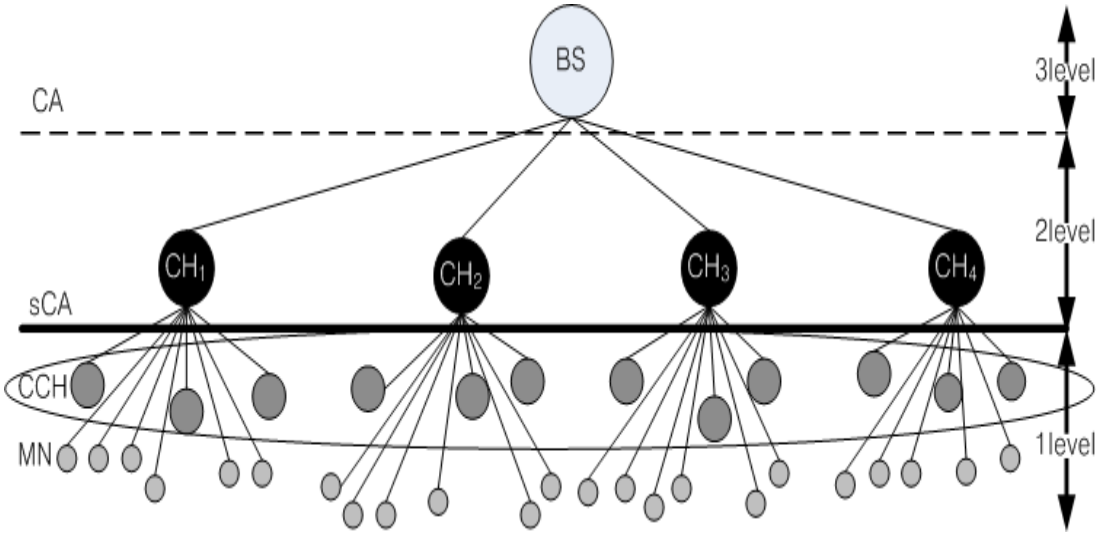


Figure 1. Our Proposed Model

Figure 1 shows the structure of our proposed model. This model is applicable to both single-hop and multi-hop communications of cluster head. Cluster heads who reside in the neighbor of base station is one-hop form base station, whereas cluster heads who reside more than one-hop form base station communicate multi-hops to base station by using the information of neighbor nodes of base station. As we use the hierarchical model in which base station serves as the CA and needs only authenticate the cluster heads to guarantee the security, this reduced the overhead of message.

In the same time, in order to authenticate nodes within its cluster, the cluster head firstly receives the JOIN messages from nodes then transmits these to base station (CA), and base station validates whether it's a valid node by inquiring from the database (DB) server.

In our proposed model, cluster head operates as the medium between authentications of base station and nodes for authentication. This model consists of base station who acts as CA, cluster head who acts as sub-CA (sCA) and member node who joins to cluster head. Cluster head is authorized a sub-CA after being authenticated by base station. Furthermore the security among cluster heads can be guaranteed without multi-hop mutual authentication between cluster heads. Member node is authenticated finally by base station through cluster head as the medium. In the situation where member node is not a valid node, Base station notifies the cluster head that this member node is an attacker and then cluster head broadcasts ID of the attacker to all nodes to avoid communication with it.

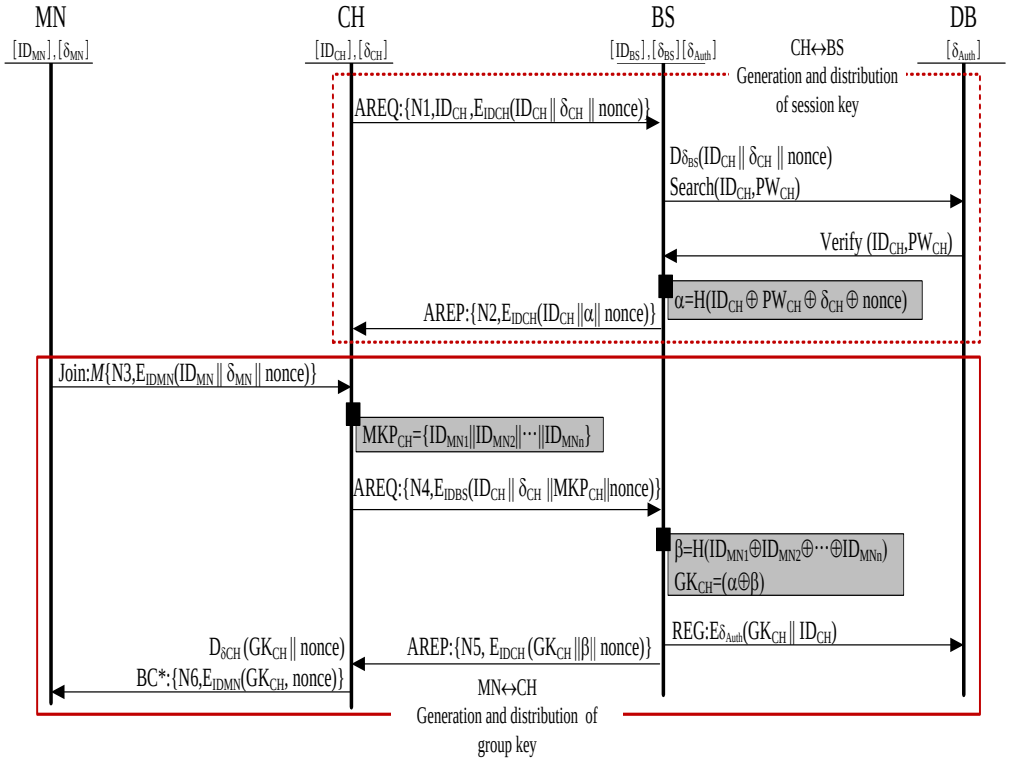


Figure 2. Group Key Generation and Distribution

Figure 2 describes the process of the generation of session key and group key for authentication. Session key (α_{CH}) is used for secure communication between cluster head and member node. Table 1 explains the symbols used in Figure 2.

Table 1. Symbol Description

Symbol	Description
ID_{CH}	ID of ith cluster head
δ_{CH}	Private information of ith cluster head
α_{CH}	Session key between cluster head and member node
none	Round number for message refreshment
PW_{CH}	Password of ith cluster head
GK_{CH}	Group key for secure communication between clusters
N_i	Seed value
ID_{MN}	ID of member node
MKP_{CH}	Key pool of member node
$EM(0, ID_{CH})$	Emergency broadcast for ID of attacker

3.2 Session Key Management between Base Station and Cluster Head

Step 1. Authentication Request Phase

Cluster head sends AREQ message to base station for authentication requesting. The message includes: ID of cluster head, seed value N1, private information value encrypted by message (δ_{CH}) and random value none to avoid message reply.

$$CH \rightarrow BS : AREQ\{N1, ID_{GH}, E_{ID_{GH}}(ID_{GH} \parallel \delta_{GH} \parallel none)\}$$

Step 2. Validation and Search

Based station authenticates cluster head with the message received from cluster head. Base Station transmits AREQ message to authentication DB server using search-query, and DB searches the Key Pair (ID, password) of cluster head. If the ID exists, the sent cluster head is valid. The authentication DB sends a repVerify message to base station which includes the private information of the requested node. If there isn't the Key Pair of the requested ID, cluster head is not a valid node. In this situation, cluster head information (ID) is broadcast to all nodes with an emergency message (0).

$$BS \rightarrow DB : reqSearch(ID_{GH}, PW_{GH})$$
$$if\ match$$
$$DB \rightarrow BS : repVerify(ID_{GH}, \delta_{GH}, PW_{GH})$$
$$if\ notmatch$$
$$BC^* : EM(0, ID_{GH})$$

Step 3. Session Key Generation

Base station receives the repVerify message from DB and generates session key based repVerify message (α_{CH}). Session key is generated by do the hash function to ID of cluster head (ID_{CH}), password of cluster head (PW_{CH}), private value (δ_{CH}) and random number (*none*) and then sent cluster head with a Authentication Response (AREP) message.

$$BS : \alpha_{CH} = H(ID_{CH_i} \oplus PW_{CH_i} \oplus \delta_{CH} \oplus none)$$
$$BS \rightarrow CH : AREP\{N2, E_{ID_{CH}}(ID_{CH} \parallel \alpha_{CH} \parallel none)\}$$

In the above (step1) to (step 3), IDE-based message is transmit. Cluster head gets authenticated by base station and is assigned a session key for secure communication between cluster heads. Every time when cluster head is changed, the session key needs to be updated.

3.3 Group Key Generation between Member Node and Cluster Head

Step 1. Member Node Authentication

Group Key (GK_{CH}) used in communication between cluster head and member node is generated as the following. Member node sends a join message to cluster head. Join message consists of two parts. One is encryption of ID, private information value, random number

with ID, the other one is seed value to avoid message reply. Cluster head collects the Join messages from member nodes and generates Member node Key Pool (MKP_{CH}).

$$MN \rightarrow CH : Join\{N_3, E_{ID_{MN}}(ID_{MN} || \delta_{MN} || none)\}$$
$$CH : MKP_{CH}\{ID_{MN_1} || ID_{MN_2} || ... || ID_{MN_n}\}$$

Step 2. Group Key Generation

Cluster head sends the member node authentication request message AREQMN to base station.

$$CH \rightarrow BS : AREQ_{MN}\{N_4, E_{ID_{CH}}(ID_{CH} \| \delta_{CH} \| MKP_{CH} \| none)\}$$
$$BS : \beta = H\{ID_{MN_1} \oplus ID_{MN_2} \oplus ... \oplus ID_{MN_n}\}$$
$$GK_{CH} = (\alpha \oplus \beta)$$

Step 3. Group Key Distribution

In order to transmit the group key, base station sends an authentication request response (AREPMN) message to cluster head. Group key is sent using a message encrypted by the ID of cluster head. Cluster head receives the group key from base station then resent it to member node. In this step cluster head broadcasts the encrypted group key message to member nodes.

$$BS \rightarrow CH : AREQ_{MN}\{N_6, E_{ID_{CH}}(GK_{CH} \| \delta_{CH} \| \| none)\}$$
$$CH \rightarrow \ *: \ BS\{N_6, E_{ID_{MN}}(GK_{CH}, \beta)\}$$

Group key is transmitted from cluster head to member node through the above (step.1) ~ (step. 3). Similar to existing mechanisms, in our proposed protocol key generation works are all completed in base station. Different to direct communication between member node and base station, authentication and key distribution of member node is through a hierarchical structure, in which member node communicates with cluster head while cluster head communicates with base station.

4. Simulation Results and Analysis

In this section, in order to evaluate the performance of our proposed protocol, we analyze the cost of creating the node authentication key and the communication cost of data transmission for authentication key compared with AM-E [12]. We also evaluate the security of the proposed mechanism.

4.1 Simulation Environment

Table 2 lists the definitions of system environment parameters and variables for our simulation. We assume that energy consumption for our simulation. We assume that energy consumption for all nodes in the active mode.

Table 2. Applications in each class

System Environment	Description
CPU	ATmega128 L, f=8Mhz
Flash memory	128Kbytes
ROM/RAM	4Kbytes/36Kbytes
Network size	100m*100M
Location of BS	50m*50m
Energy consumption of circuit	50nJ/bit
Data aggregation	50nJ/bit
Radius of communication	(multi)10m/(single)20m
Number of cluster head	2
Maximum hop count	3
Total number of node	1,000
Between node distance	10m
Message of length	3840bit
Loss in free space	10pJ/bit
Encryption / Decryption	0.64ms /0.42ms
Delay loss	2/4.3
Round	2000
Total energy consumption	50/ 150J

4.2 Simulation Results

We compared the cost for creating node authentication keys and the communication cost for data transmission of authentication keys with AM-E [12]. The whole energy consumption spent for establishment of authentication keys between cluster head and member node is as in (equation 2).

In our simulation, energy consumption for authentication key establishment is calculated based on the energy consumption in cluster head (equation 3) and the energy consumption in member nodes (equation 4) in one round. Furthermore, we analyzed the energy consumption (equation 5, 6) in communications for authentication key between cluster head and member node and the energy consumption within the cluster (equation 7).

4.2.1 Analysis of Energy Consumption: To analyze the energy efficiency of the proposed protocol, energy consumption for authentication key establishment in member node and cluster head is respectively defined in (equation 3) and (equation 4). (Equation 3) is the energy consumption in cluster head, while (equation 4) is the energy consumption in member node. Based on (equation 3) and (equation 4), (equation 2) is the whole energy consumption for authentication key establishment in a cluster.

$$AE_{cluster} = \sum_{i=1}^{r} (AE_{CH} + AE_{MN}) \quad \textbf{(2)}$$

Equation (3) is the energy consumption which is needed in the multi-hop communication of cluster head.

$$AE_{CH} = T\left[(2\delta + \mu R^k)\left(\frac{d^2}{R^2 - 1} \right) + \left(1 + \mu R^2\right) \right] \quad \textbf{(3)}$$

(Equation 4) describes the energy consumption for the single-hop communication from member node to cluster head in T-cycle. Based on (equation 2) to (equation 4), we can measure the energy consumption for authentication key establishment.

From Figure 3, we can find that with the communication distance between member node and cluster head getting further, energy consumption for authentication key establishment gets increased.

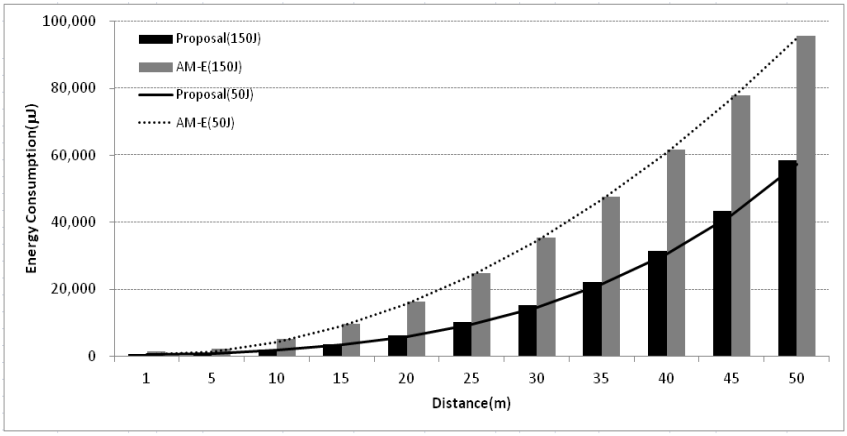


Figure 3. The Communication Distance between MN and CH Getting

Figure 4 displays the energy consumption value with the change of communication distance in a cluster. According to the results, we draw the conclusion that energy consumption increases with the increasing of communication distance.

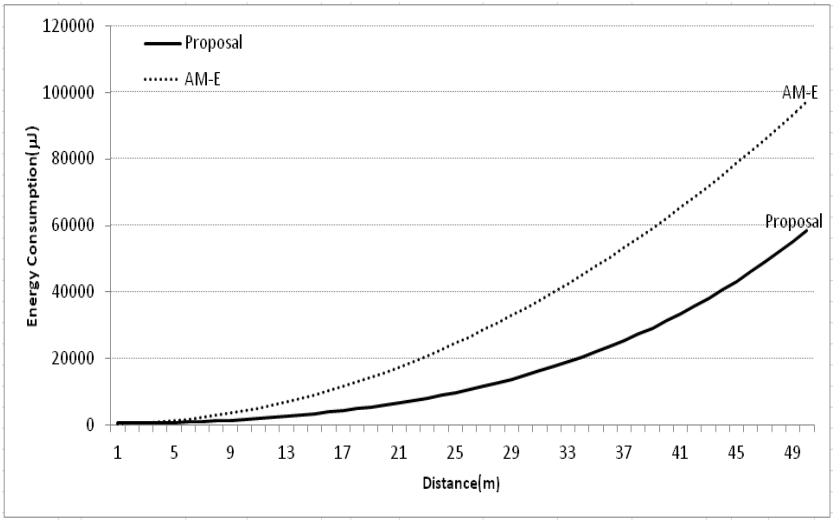


Figure 4. The Energy Consumption Value with the Change of Communication Distance in a Cluster

In the next, we calculated the energy consumption for message communication using the authentication key. In a round, the energy consumption in cluster head for the communication is as defined as in (equation 5), whereas the energy consumption in member node for the communication is defined in (equation 6).

$$E_{CH} = M \times E_{elec}\left(\frac{n}{k} - 1\right) + M \times \frac{n}{k} + M \times e_{fs} {d_{BS}}^2 \quad \textbf{(5)}$$

$$E_{MNs} = M \times E_{elec} + M \times e_{fs} \times {d_{CH}}^2 \quad \textbf{(6)}$$

Based on equation (5) and (6), the whole energy consumption for communication in a cluster can be calculated as in equation (7).

$$E_{cluster} = E_{CH} + \left(\frac{n}{k} - 1\right) E_{MNs} \quad \textbf{(7)}$$

Summarizing the above equations from (2) to (7), we can calculate the whole energy consumption in a round, which includes the energy consumption for key establishment and for message communication, in both cluster head and member node. The result is calculated as equation (8):

$$E_{tot} = M\left\{2nE_{elec} + nE_{DA} + e_{fs}\left(k{d_{BS}}^2 + n{d_{CH}}^2\right)\right\} \quad \textbf{(8)}$$

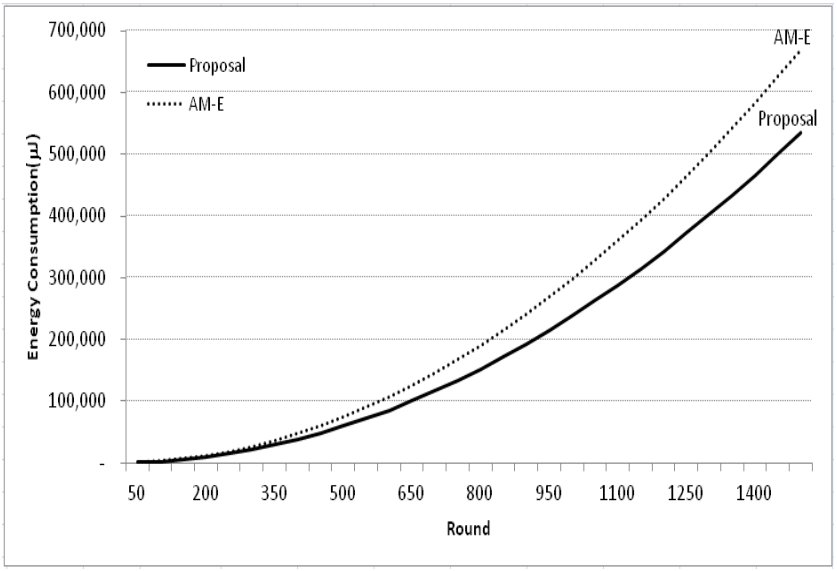


Figure 5. Energy Consumption of all Participated Nodes for Authentication in Different Rounds

Figure 5 shows the number of nodes alive in the network during the whole lifetime. We can discovery that in the same rounds our proposed protocol has lower energy consumption than AM-E protocol [12], while in the same network lifetime there are more nodes alive in the network than in AM-E [12].

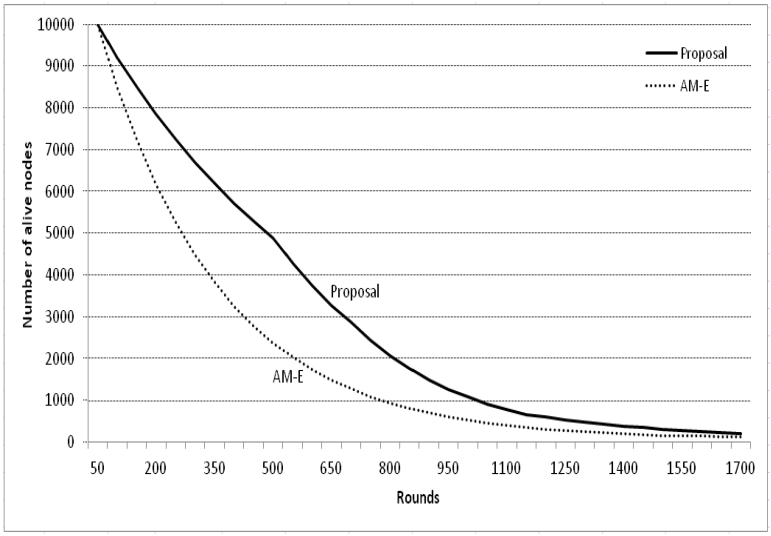


Figure 6. The Number of Nodes Alive in the Network during the Whole Lifetime

In this paper, member node and cluster head directly communicate with each other (single –hop communication), whereas cluster head and base station use the multi-hop (max h=3) communication to each other. By this way, the communication time is increased than AM-E [12]. Therefore, the lifetime of our proposed protocol gets prolonged too.

4.2.2 Analysis of Security

(a) Secret Key Attack using Tapping

Attacker can obtain the secret key by tapping the messages sent or received for session key generation. In this proposed protocol, it's not possible for attacker to calculate the password (PW_{CH}) and secret key (δ_{CH}) of nodes, which are needed in the generation of session key (α_{CH}). With tapping information the attacker can only obtain the ID (ID_{CH}) while not the secret key (δ_{CH}) of nodes. Without the secret key, the attacker can't decrypt the encrypted message.

In some case the attacker can possibly gain the secret key of nodes. But the password of node, which is necessary for session key generation, is only obtained from the authentication DB server. Due to this, it's impossible for the attacker to generate the session key ($\alpha_{CH} = (ID_{CH} \oplus PW_{CH} \oplus \delta_{CH} \oplus none)$). So our proposed protocol provided confidentialness for session key establishment, which aims at secure communications among nodes, and IDE-based encryption communication.

(b) Attack to Modify Message

Message modulation attack is that the attacker modifies the gained message and then resends the modified message or passes authentication with this fade message. In our protocol, to guarantee the communications between member node and cluster head and between cluster head and base station both in secure ways, session key and group key is established and the IDE-based encrypted message is transmitted. As a result, even if the encrypted message is modified by the attacker, the receiver can't decrypt this modified message, so the message modulation attack gets ineffective.

(c) Attack to Message Replay

Message replay attack is that an attacker uses the previous information again to obtain authentication or key agreement. In our proposed paper, in order to keep the refreshment of the message, we transmit the random number $N1, N2, N3, N4, N5, N6$ with the encrypted message together. Even if the attacker acquires the message, replay attack using the previous information is not valid any more. This way needs not time synchronization of each node, in the same time avoids the replay attack.

5. Conclusion

In this paper, we proposed an IDE-based hierarchical node authentication mechanism for secure data transmission in ad-hoc network. In previous works for ad-hoc network, when nodes transmit collected data base station or cluster head, the data needs not be authenticated, so the safety of transmitted data is not guaranteed. After that, with account of the characteristics of ad-hoc network, various methods that authenticate the participated nodes in communication are proposed.

In these mechanisms, AREQ/AREP message for node authentication consume much energy and the direct communications between base station and sink nodes also need much energy, this causes large burden for nodes have very limited energy. And it also influents the essential works of nodes, it is data sense and collection. Therefore, with consideration that energy consumption is proportional to size of message and distance of nodes, we utilize a clustering hierarchical structure, where cluster heads act as the medium between base station and normal nodes. Base station takes role of the CA for all nodes. Before all nodes are authenticated, cluster head should get the authentication of base station. If the authentication is passed, the cluster head becomes sub-CA (sCA) to authenticate remained nodes.

In our proposed protocol, by using IDE-based hierarchical node authentication mechanism the whole energy consumption in ad-hoc network obtains minimized. Furthermore, because only authenticated nodes can take part in the communication, the security of data is assured. From the results of simulation , we can find that our proposed protocol can provide same level security as in AM-E [12], while energy consumption in one round decreased about 34% and the number of nodes alive increased about 20%, in the same time, round number for network lifetime increased about 300 rounds. By analyzing the results, the energy consumption rate decreases about 29%.

In a summary, our proposed protocol not only guarantees the same security, but also efficiently reduces energy consumption compared with previous works. The future works include researches on advanced secure mechanism and various attacks in ad-hoc network for secure data transmission.

References

[1] Ke W, Basu P, Abu Ayyash S and Little TDC, “Attribute Based Hierarchical Clustering in Wireless Sensor Networks”, MCL Technical Report No. 03-24-2003, **(2003)**.
[2] Bandyopadhyay S and Coyle EJ, “An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks”, INFOCOM2003, SanFrancisco , USA, **(2003)** April 1-3.
[3] Eschenauer L and Gligor VD, “A key management scheme for distributed sensor networks”, In 9th ACM conference on computer and communications security, New York, **(2002)**.
[4] Silva RMS, Pereira NSA and Nunes MS, “Applicability Drawbacks of Probabilistic Key Management Schemes for Real World Applications of Wireless Sensor Networks”, Proceeding of the Third International Conference on Wireless and Mobile Communication (ICWMC'07), **(2007)** March 4-9.
[5] Perrig A, Szewczyk R, Wen V, Culler D and Tygar JD, “SPINS: Security Protocols for Sensor Networks, Wireless Networks”, vol. 8. no. 5, Rome, Italy, **(2001)** 16-21 July.

[6] Huang Q, Cukier J, Kobauashi H, Liu B and Zhang J, "Fast Authenticated Key Establishment Protocols for Self-organizing Sensor Networks", In Proc. of the 2nd SCM International Conference on Wireless Sensor Networks and Applications, **(2003)** September.
[7] Zhu S, Setia S and Jajodia S, "LEAP: Efficient Security Mechanisms for Large-scale Distributed Sensor Networks", Proceedings of the 10th ACM Conference on Computer and Communication Security, CCS 2003, Oct 27-30,Washington, DC, USA, **(2003)** October 27-30.
[8] Chan H and Perrig A, "PIKE:Peer Intermediaries for Key Establishment in Sensor Networks", IEEE Infocom, vol. 1, Miami , **(2005)** March 13-17.
[9] Juang WS, "Efficient User Authentication and Key Agreement in Wireless Sensor Networks", WISA 2007, LNCS 4298, **(2007)**, pp. 15-29, Springer-Verlag.
[10] Ibriq J and Mahgoub I, "A Hierarchical key establishment scheme or Wireless sensor networks", Proceedings of 21st International conference on advanced Networking and applications(AINA07), Niagara Falls, Canada, **(2007)** May 21-23.
[11] Huyen TT, Huh EN, "A reliable 2-mode authentication framework for Ubiquitous sensor network", Journal of Korean Society for Internet Information, KOREA, **(2008)**.
[12] Kim B, Lim L, Choi J and Shin Y, "A Study on Node Authentication Mechanism using Sensor Node's Energy Value in WSN", In journal of the institute of electronics engineers of Korea, vol. 48, no. 2, **(2011)**.
[13] Ibriq J and Mahagoub I, "Cluster-based routing in wireless sensor network: Issues and Challenges", SPECTS'04, San Jose, USA, **(2004)** July 25-29.
[14] Eschenauer L and Gligor VD, "A key management scheme for distributed sensor networks", In 9th ACM conference on computer and communications security, Washington DC, USA, **(2002)** November.

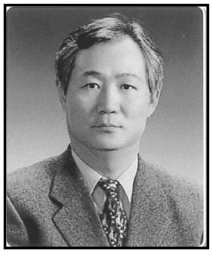
Authors

Youngbok Cho received the M.S. degree in the department of computer science from Chungbuk National University, Korea, in August 2003. She is currently in the process of a Ph.D. Her research interests include mobile ad hoc network and wireless sensor networks.

E-mail: bogicho@cbnu.ac.kr

Ning Sun received the BS in Mechanical and Automotive Engineering from Shandong Polytechnic University, China and MS in Computer Science from Chungbuk National University, Republic of Korea in 2000 and 2008 respectively. She is pursuing the Ph.D degree in Computer Science from Chungbuk National University, Korea. Her current research interests include wireless sensor networks, Mobile Adhoc networks, Network Security, Network Applications, Ubiquitous Computing.

E-mail: sunn2001@hotmail.com



Sang-Ho Lee was born in Pyoung-Taek, Korea in 1953. He received the B.S. degree in the department of computer science, Soongsil National University in February 1976. He received the M.S. degree in the department of computer science, Soongsil National University in February 1981. He received the P.H.D. degree in the department of computer science, Soongsil National University in February 1989. He is currently working professor in the department of electrical and electronics engineering, Chungbuk National University. His research interests also include Protocol Engineering, Network Security, Network Management and Network Architecture

E-mail : shlee@chungbuk.ac.kr