A Black Hole Detection Protocol Design based on a Mutual Authentication Scheme on VANET

ByungKwan Lee[1] and EunHee Jeong[2*]
[1]Department of Computer Engineering, Catholic Kwandong University
Gangneung-si, Gangwon-do South Korea
[e-mail: bklee@cku.ac.kr]
[2]Department of Regional Economics, Kangwon National University
Samcheok-si, Gangwon-do South Korea
[e-mail: jeongeh@kangwon.ac.kr]
*Corresponding author: EunHee Jeong

Received August 31, 2015; revised December 7, 2015; accepted March 10, 2016; published March 31, 2016

Abstract

This paper proposes "A Black Hole Detection Protocol Design based on a Mutual Authentication Scheme on VANET." It consists of the Mutual Authentication Scheme (MAS) that processes a Mutual Authentication by transferring messages among a Gateway Node, a Sensor Node, and a User Node and the Black Hole Detection Protocol (BHDP) which detects a Non-Authentication Node by using the Session Key computed in the MAS and a Black Hole by using the Broadcasting Table. Therefore, the MAS can reduce the operation count of hash functions more than the existing scheme and protect a privacy from an eavesdropping attack and an information exposure by hashing a nonce and user's ID and password. In addition, the MAS prevents a replay attack by using the randomly generated nonce and the time stamp. The BHDP improves Packet Delivery ratio and Throughput more than the AODV with Black hole by 4.79% and 38.28Kbps. Also, it improves Packet Delivery ratio and Throughput more than the IDSAODV by 1.53% and 10.45Kbps. Hence it makes VANET more safe and reliable.

Keywords: Mutual Authentication, Black Hole Detection Protocol, Broadcasting Table, Session Key

A preliminary version of this paper was presented at APIC-IST 2015, and selected as an outstanding paper. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2013R1A1A2062415). This work was supported by research fund of Catholic Kwandong University.

http://dx.doi.org/10.3837/tiis.2016.03.032 **ISSN : 1976-7277**

1. Introduction

Because of the development of IoT and Smart devices, such heterogenous Ad Hoc or Wireless Sensor Network as MANET and VANET is being built easily. The supply expansion of intelligent terminals like a smart phone provides us with an affirmative opportunity to share and use information. But, the supply expansion of intelligent terminals is providing us with a negative phenomenon that illegal information is acquired and the acquired information is used maliciously. Particularly, it causes serious consequences to the MANET environment that makes it temporarily, not to use a communication infrastructure.

A Black Hole Attack to lose data transfer function is a threatening information attack to MANET and VANET. If a Black Hole attack happens to the VANET, the non-transmission of information can cause the traffic congestion and the serious problems like another accident.

This paper proposes “A Black Hole Detection Protocol Design based on a Mutual Authentication Scheme on VANET.” It consists of the Mutual Authentication Scheme (MAS) that processes a Mutual Authentication by transferring messages among a Gate Way Node (GWN), a Sensor Node(=RSU), and a User Node(=Vehicle) and the Black Hole Detection Protocol (BHDP) which detects a Non-Authentication Node by using a Session Key (SK) computed in the MAS and a Black Hole Node on VANET by using the Broadcasting Table. Therefore, the MAS can reduce the operation count of hash functions more than the existing scheme and protect a privacy from an eavesdropping attack and an information exposure by hashing a nonce and user’s ID and password.

The remainder of this paper is organized as follows. Chapter2 discusses the related works. Chapter3 proposes a Black Hole Detection Protocol(BHDP) Design based on Mutual Authentication. Chapter4 analyzes and estimates its performance. In the chapter 5, our conclusion is described.

2. Related Work

2.1 VANET

A Vehicular Ad hoc Network (VANET) provides convenient wireless network services. In addition, in VANET, vehicles can exchange and receive the traffic information [1-2]. VANET can enhance traffic safety and improve traffic efficiency by transmitting the messages with traffic information and road condition information [3-4].

Hence, traffic accidents and jams can be significantly diminished. Since inexpensive wireless devices are available, they can be installed at various RSUs, such as road signs and traffic lights. The primary objective of VANET is to provide real-time exchange of messages between vehicles to ensure safety. However, the security of VANET is important because messages can be tampered or counterfeited by malicious nodes during transmission [5-7].

2.2 AODV

Ad hoc On-demand Distance Vector (AODV) [8-10] routing protocol is widely used in ad hoc networks. Route discovery operation is used to discover the route by using Route Request (RREQ) and Route Reply (RREP) control messages. **Fig. 1** shows the message structure of AODV.

Type	Flags	Reserved	Hop Count
RREQ(Broadcast)			
Destination IP address			
Destination sequence number			
Source IP address			
Source sequence number			

(a) RREQ message

Type	A	Reserved	Hop Count
Destination IP address			
Destination sequence number			
Source IP address			
Source sequence number			

(b) RREP message

Fig. 1. The message structure of AODV

A source node broadcasts a RREQ when the data is required to send to a destination node. A route is created when each intermediate node receives RREQ if the intermediate node is not the destination node and never received this RREQ before, it will broadcast the RREQ. The RREP is unicast to the source node when the receiving node is the destination node. The source node will check and choose the shorted path when it receives more than one RREP. The route is only updated if the hop count in RREP is smaller than the existing route in route table [10-11].

AODV has more vulnerable to attack. Because of AODV lacking a mechanism to handle or detect the false information in RREQ and RREP, this kind of attack can easily occur in ad hoc networks [10].

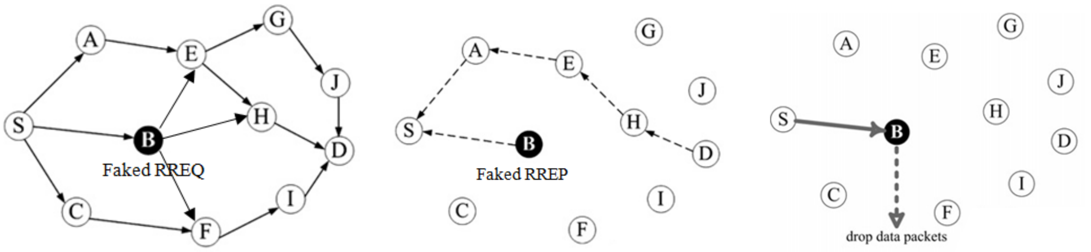
This paper proposes to detect a Black hole Attack by adding Session key to RREQ/RREP message and by using the Broadcasting Table.

2.3 Black Hole Attack

In networking, black holes refer to places in the network where incoming traffic is silently discarded (or "dropped"), without informing the source that the data did not reach its destination. These black hole nodes are invisible and can only be detected by monitoring the lost traffic. A Black hole attack is one of the active DoS attacks possible in MANETs.

In this attack, a malicious node sends a *false* RREP packet to a source node that initiated the route discovery, in order to pose itself as a destination node or an immediate neighbor to the actual destination node. In such a case, the source node would forward its entire data packets to the malicious node, which originally was intended for the genuine destination. The malicious node, eventually may never forward any of the data packets to the genuine destination. As a result, therefore, the source and the destination nodes became unable to communicate with each other [12-13].

Fig. 2 depicts the behavior of a black hole attack, wherein source node S is intended to establish a route to destination node D. In an AODV routing protocol, node S would broadcast a RREQ packet to search for destination node D; the normal intermediate nodes would receive and continuously broadcast the RREQ, rather than the Black hole node. As shown in **Fig. 2(a)**, the Black hole node would directly reply through an RREP with an extremely large sequence number and hop count of 1 to source node S. When receiving RREQs from normal nodes, the destination node D would also select a route with a minimal hop count, and then, return a RREP packet, as shown in **Fig. 2(b)**. According to the AODV design, a source node would select the latest (largest sequence number) and shortest route (minimal hop count) to send data packets upon receipt of several RREPs packets. Thus, a route via a Black hole node would be selected by node S. The Black hole node will then eavesdrop, or directly drop the received data packets, as shown in **Fig. 2(c)** [14].



(a) RREQ Black hole attack (b) RREP Black hole attack (c) drop data packets

Fig. 2. Black hole attack

S.DOKURER [15] proposed IDSAODV this method modified in AODV protocol that implemented minimize the effect of malicious node. This method implemented by modified in the routing update mechanism in AODV protocol. IDSAODV tries to eliminate the effect of the Black hole attack by ignore the first route in the routing update process. The first RREP message arrived with shortest route to the destination node from the malicious node. IDSAODV switched to the second route, The Black hole node increasing the date loss to 89% when used IDSAODV decreased the data loss to 67% this solution reduce the Black effect by 22% as packet loss [16].

Ankita Chaturvedi, Sanjiv Sharma [17] proposed IIDSAODV is based on checking the second RREP message and uses the sequence number is a 32 bit unsigned integer the Highest value (HSN). Check second RREP, the difference between the broadcasted and received destination sequence number is calculated and compared to the half of the highest possible sequence number (HSN). The difference should be less than or equal to (HSN/2). If second RREP pass then only the source node switches to this path. If checked fails the source node continue to send the data through the path by first RREP. In Black hole decrease the PDR of AODV by 83.79%, in case IDSAODV and IIDSAODV increase by 40.41% and 78.16%. Decrease throughput of AODV by 77.86%, in case IDSAODV and IIDSAODV increase by 20.66% and 73.59%. Decrease end-to-end delay of AODV by 88.74%, in case IDSAOD and IIDSAODV increase by 44.15% and 71.61% [16].

DPRAODV [18] proposed method that based authenticate the RREP sequence number. RREP_seq_no is higher than the threshold value. Threshold value is dynamically updated, the value of RREP_seq_no is found to be higher than the threshold value, the node is suspected to be malicious and it adds the node to the black list. It sends a new control packet, ALARM to its neighbors. The neighboring nodes know that RREP packet from the node is to be discarded. It simply ignores the node and does not receive reply from that node again [16].

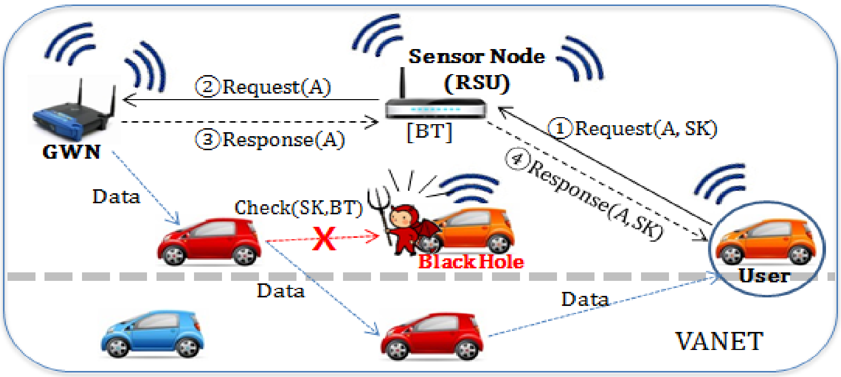
Thus, this paper proposes a Black Hole Detection Protocol design based on a Mutual Authentication Scheme. That protocol detects a Black Hole happening because of the fake of the RREQ and RREP by checking the Time Stamp and SK of a Broadcasting Table and the SK of an RREQ and RREP message.

3. Black Hole Detection Protocol Design

This paper proposes “A Black Hole Detection Protocol Design based on a Mutual Authentication Scheme on VANET”. It consists of a GateWay Node (GWN), a Sensor Node(=RSU), and a User Node(=Vehicle) like Fig. 3.

The GWN is responsible for the gateway of VANET and manages the ID and shared key of a Sensor Node(=RSU). When the Sensor Node registers a User Node or collects data, it is responsible for the connection of the GWN to the User Node and manages a Broadcasting Table (BT).

The GWN, Sensor Node, and User Node of VANET confirms their identity with MAS and generates a Session Key (SK) between the Sensor Node and the User Node. The Sensor Node detects a Non-Authentication Node with the SK and a Black Hole Node with the BT. The User Node transfers data to a Destination Node safely after removing these threatening elements.



*A:Authentication, SK:Session Key, BT:Broadcasting Table

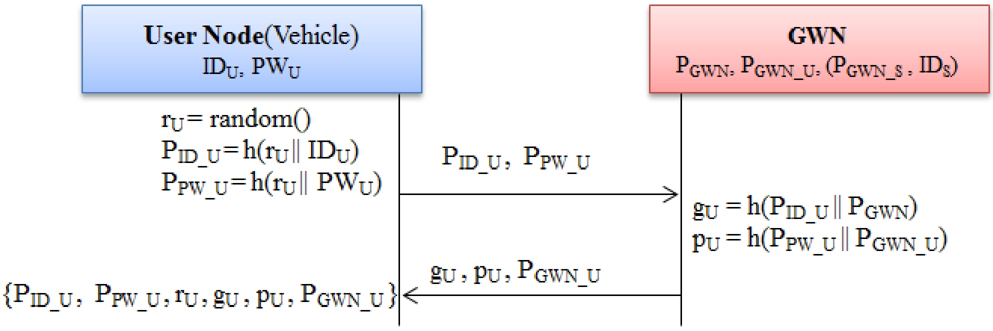
-------> Data transmision

Fig. 3. The total flowchart

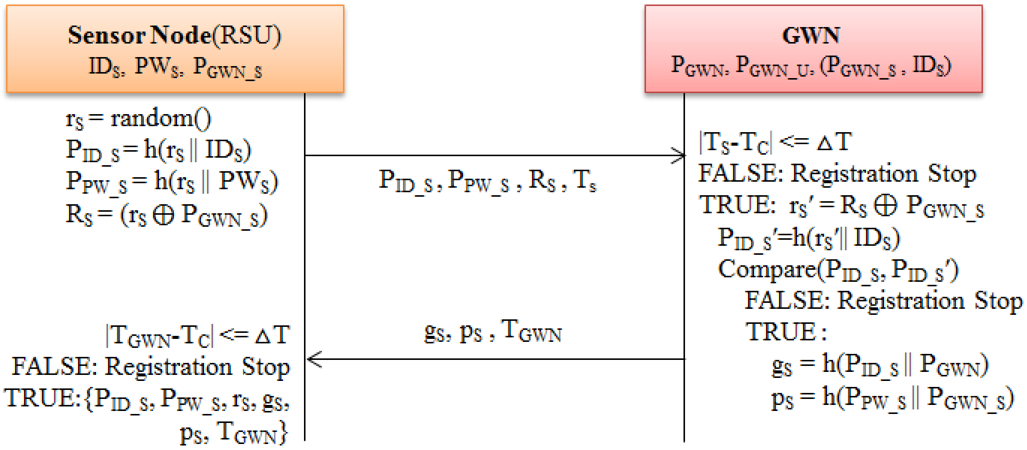
3.1 A Registration Phase

In the registration of the User Node in this paper, because the value computed by a hash function, not by a user’s ID and password is used, the exposure of a user’s ID and password is prevented and his privacy is protected.

Fig. 4 shows the procedure of a registration phase [19]. The lengthe of ID and password that are 8byte, and h means SHA-1 Hash function.



(a) User Node registration


Sensor Node(RSU)
ID_S, PW_S, P_{GWN_S}
GWN
P_{GWN}, P_{GWN_U}, (P_{GWN_S} , ID_S)
r_S = random()
P_{ID_S} = h(r_S || ID_S)
P_{PW_S} = h(r_S || PW_S)
R_S = ($r_S \oplus P_{GWN\_S}$)
P_{ID_S} , P_{PW_S} , R_S , T_s
|T_S-T_C| <= ΔT
FALSE: Registration Stop
TRUE: r_S' = $R_S \oplus P_{GWN\_S}$
P_{ID_S}'=h(r_S'|| ID_S)
Compare(P_{ID_S}, P_{ID_S}')
FALSE: Registration Stop
TRUE :
g_S = h(P_{ID_S} || P_{GWN})
p_S = h(P_{PW_S} || P_{GWN_S})
g_S, p_S , T_{GWN}
|T_{GWN}-T_C| <= ΔT
FALSE: Registration Stop
TRUE:{P_{ID_S}, P_{PW_S}, r_S, g_S, p_S, T_{GWN}}

(b) Sensor Node registration

Fig. 4. The registration procedure

(1) A Registration of a User Node(=Vehicle)

A User Node generates a nonce r_U randomly and computes P_{ID_U}(=h(r_U || ID_U)) by hashing the r_U and the User Node ID_U. The User Node computes P_{PW_U}(=h(r_U || PW_U)) by hashing a password PW_u and r_U and delivers {P_{ID_U}, P_{PW_U}} to the GWN.

The GWN computes g_U(=h(P_{ID_U}||P_{GWN}) by hashing the transferred User Node's P_{ID_U} and its own password $P_{GWN.}$ and p_U(=h(P_{PW_U} || P_{GWN_U})) by hashing the transferred User's P_{PW_U} and User's shared key $P_{GWN\_U.}$ Then, the GWN transfers {g_U, p_U, P_{GWN_U}} to the user Node.

The User Node stores in its memory the values {P_{ID_U}, P_{PW_U}, r_U, g_U, p_U, P_{GWN_U}}.

(2) A Registration of the Sensor Node(=RSU)

The Sensor Node has ID_S, PW_S and the GWN's Shared key P_{GWN_S}. It computes the P_{ID_S} (=h(r_S||ID_S)) by hashing a randomly generated nonce r_S and ID_S, the P_{PW_S}(=h(r_S||PW_S)) by hashing r_S and PW_S, and the R_S(=$r_S \oplus P_{GWN\_S}$) by XORing nonce r_S and $P_{GWN\text{-}S.}$ Because of these, the exposure of r_S, ID_S, and PW_S values are protected. And the Sensor Node transfers these computed values {P_{ID_S}, P_{PW_S}, R_S, T_S} to the GWN. Here, T_S means the time Stamp when the Sensor Node transfers messages.

The GWN checks the T_S representing the time when a message is transferred. If a critical time ΔT is exceeded, the GWN closes the registration of the Sensor Node. If a message is transferred within ΔT, the GWN computes the nonce r_S'(=$R_S \oplus P_{GWN\_S}$) to authenticate the integrity of the message transferred from the Sensor Node and the P_{ID_S}'(=h(r_S'||ID_S)) by hashing the r_S' and ID_S(Sensor Node' ID). Then, the GWN compares the P_{ID_S} transferred from the Sensor Node with the P_{ID_S}'. If the comparison is false, the GWN closes the registration of the Sensor Node. It it is true, the GWN computes the g_S(=h(P_{ID_S}||P_{GWN})) and p_S(=h(P_{PW_S}||P_{GWN_S}) necessary for a Mutual Authentication. Then, the GWN transfers to the Sensor Node the {g_S, p_S, T_{GWN}} necessary for a Mutual Authentication.

The Sensor Node checks the T_{GWN} when a message is transferred. If a critical time ΔT is exceeded, the Sensor Node closes the registration of a User Node. If a message is transferred within ΔT, the Sensor Node stores the {P_{ID_S}, P_{PW_S}, r_S, g_S, p_S,T_{GWN}} in its memory.

3.2 A Mutual Authentication Phase

The Mutual Authentication of this paper makes the User Node, the Sensor Node, and the

GWN confirm their identify simultaneously. **Fig. 5** shows the procedure of mutual authentication phase [19].

The Sensor Node and User Node stores in their memory each $\{ID_U, PW_U, P_{ID\_U}, P_{PW\_U}, r_U, g_U, p_U, P_{GWN\_U}\}$, and $\{ID_S, PW_S, P_{GWN\_S}, P_{ID\_S}, P_{PW\_S}, r_S, g_S, p_S, T_{GWN}\}$ after finishing the registration phase of section 2.1. The User Node, the Sensor Node, and the GWN use these values in the Mutual Authentication.

The User Node generates a nonce a_U randomly and computes a new $A_U(=a_U \oplus g_U)$ by XORing a_U and g_U. Then, the User Node computes a authentication value $MA_U(=h(P_{PW\_U} \| P_{GWN\_U} \| p_U) \oplus a_U \oplus T_U)$ for an identity authentication of the User Node and transfers $\{A_U, MA_U, T_U\}$ to the Sensor Node. Here, T_U means a Time Stamp when the User Node generates an authentication value.

The Sensor Node also computes a authentication value $MA_S(=h(ID_S \| P_{GWN\_S} \| T_{GWN}) \oplus p_S)$ for identity authentication and transfers to the GWN the value $\{A_U, MA_U, T_U, MA_S, T_S\}$ transferred from the User Node and computed by the Sensor Node.

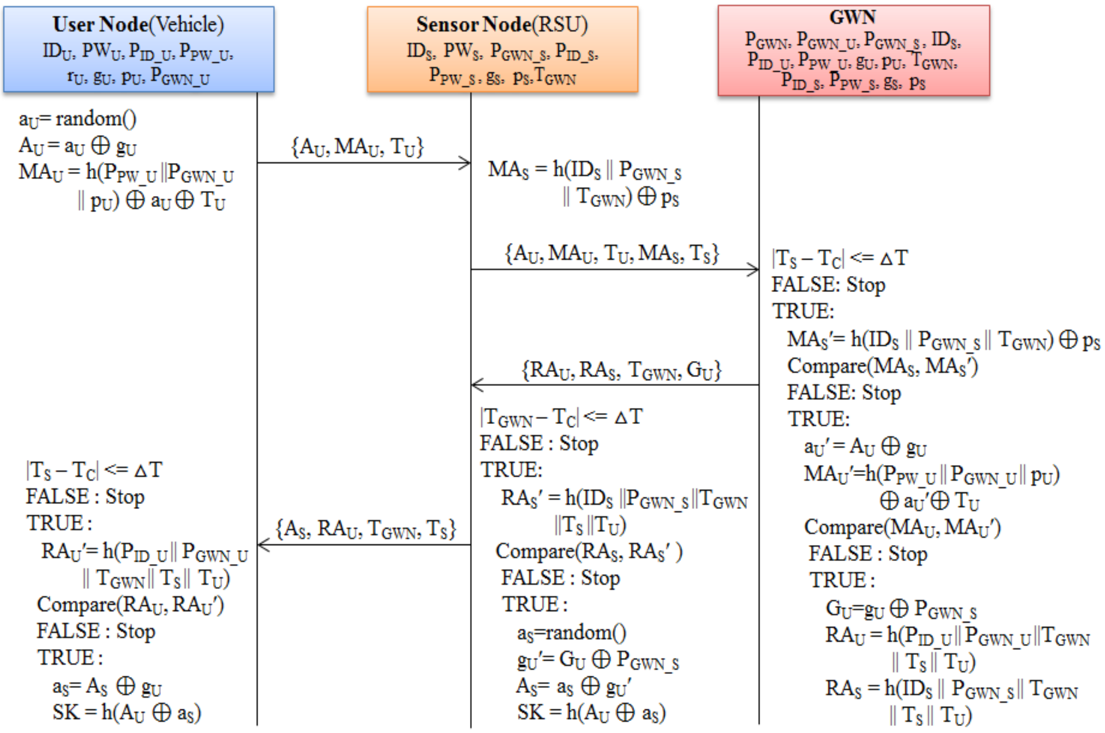

User Node(Vehicle)
$ID_U, PW_U, P_{ID\_U}, P_{PW\_U}, r_U, g_U, p_U, P_{GWN\_U}$
Sensor Node(RSU)
$ID_S, PW_S, P_{GWN\_S}, P_{ID\_S}, P_{PW\_S}, g_S, p_S, T_{GWN}$
GWN
$P_{GWN}, P_{GWN\_U}, P_{GWN\_S}, ID_S, P_{ID\_U}, P_{PW\_U}, g_U, p_U, T_{GWN}, P_{ID\_S}, P_{PW\_S}, g_S, p_S$
a_U= random()
$A_U = a_U \oplus g_U$
$MA_U = h(P_{PW\_U} \| P_{GWN\_U} \| p_U) \oplus a_U \oplus T_U$
$\{A_U, MA_U, T_U\}$
$MA_S = h(ID_S \| P_{GWN\_S} \| T_{GWN}) \oplus p_S$
$\{A_U, MA_U, T_U, MA_S, T_S\}$
$|T_S - T_C| <= \Delta T$
FALSE: Stop
TRUE:
$MA_S' = h(ID_S \| P_{GWN\_S} \| T_{GWN}) \oplus p_S$
Compare(MA_S, MA_S')
FALSE: Stop
TRUE:
$a_U' = A_U \oplus g_U$
$MA_U' = h(P_{PW\_U} \| P_{GWN\_U} \| p_U) \oplus a_U' \oplus T_U$
Compare(MA_U, MA_U')
FALSE : Stop
TRUE :
$G_U = g_U \oplus P_{GWN\_S}$
$RA_U = h(P_{ID\_U} \| P_{GWN\_U} \| T_{GWN} \| T_S \| T_U)$
$RA_S = h(ID_S \| P_{GWN\_S} \| T_{GWN} \| T_S \| T_U)$
$\{RA_U, RA_S, T_{GWN}, G_U\}$
$|T_{GWN} - T_C| <= \Delta T$
FALSE : Stop
TRUE:
$RA_S' = h(ID_S \| P_{GWN\_S} \| T_{GWN} \| T_S \| T_U)$
Compare(RA_S, RA_S')
FALSE : Stop
TRUE :
a_S=random()
$g_U' = G_U \oplus P_{GWN\_S}$
$A_S = a_S \oplus g_U'$
$SK = h(A_U \oplus a_S)$
$\{A_S, RA_U, T_{GWN}, T_S\}$
$|T_S - T_C| <= \Delta T$
FALSE : Stop
TRUE :
$RA_U' = h(P_{ID\_U} \| P_{GWN\_U} \| T_{GWN} \| T_S \| T_U)$
Compare(RA_U, RA_U')
FALSE : Stop
TRUE :
$a_S = A_S \oplus g_U$
$SK = h(A_U \oplus a_S)$

Fig. 5. The procedure of mutual authentication

The GWN confirms the time stamp T_S when a message is transferred. If a critical time ΔT is exceeded, the GWN closes a Mutual Authentication. If the message arrived within ΔT, the GWN computes the $MA_S'(=h(ID_S \| P_{GWN\_S} \| T_{GWN}) \oplus p_S)$ to confirm the authentication value of the Sensor Node and compares MA_S with MA_S'. If the comparison is false, the GWN drops all the values transferred from the Sensor Node and closes the Mutual Authentication. If it is true, the GWN decides that the Sensor Node should be reliable.

The GWN computes $a_U'(=A_U \oplus g_U)$ with the A_U transferred from the Sensor Node for the authentication of the User Node. Then, the GWN computes $MA_U'(=h(P_{PW\_U} \| P_{GWN\_U} \| p_U) \oplus a_U' \oplus T_U)$ and compares MA_U with MA_U'. If the comparison is false, the GWN drops all the values transferred from the Sensor Node and closes the Mutual Authentication. If it is true, the

GWN decides that the User Node should be reliable.

Now, the GWN computes the $G_U(=g_U \oplus P_{GWN\_S})$ necessary to generate SK. Then, the GWN computes the authentication confirmation values $RA_U(=h(P_{ID\_U}||P_{GWN\_U}||T_{GWN}||T_S|| T_U))$ of the User Node and $RA_S(=h(ID_S|| P_{GWN\_S} || T_{GWN} || T_S || T_U)$ of the Sensor Node. Here, T_{GWN} means the time stamp reset by the current time to transfer the message of the authentication confirmation values. The GWN transfers $\{RA_U, RA_S, T_{GWN}, G_U\}$ to the Sensor Node.

The Sensor Node checks the time stamp T_{GWN} when a message is transferred. If a critical time ΔT is exceeded, the Sensor Node closes a Mutual Authentication. If the message arrived within ΔT, the Sensor Node computes $RA_S'(=h(ID_S || P_{GWN\_S} || T_{GWN} || T_S || T_U)$ and verifies integrity by comparing RA_S' and $RA_{S.}$ If the comparison is false, the Sensor Node closes the Mutual Authentication. If it is true, the Sensor Node computes $g_U'(=G_U \oplus P_{GWN\_S})$ and $A_S(=a_S \oplus g_U')$ after generating a random nonce a_S. Then, The Sensor Node generates $SK(=h(A_U \oplus a_S))$ by using these values and transfers $\{A_S, RA_U, T_{GWN}, T_S\}$ to the User Node.

The User Node confirms the T_{GWN} when a message is transferred. If a critical time ΔT is exceeded, the User Node closes the Mutual Authentication. If the message arrived within ΔT, the User Node computes $RA_U'(=h(P_{ID\_U} || P_{GWN\_U} || T_{GWN} || T_S || T_U)$ and verifies integrity by comparing RA_U' with $RA_{U.}$

If the comparison is false, the User Node closes the Mutual Authentication. If it is true, the User Node computes $SK(=h(A_U \oplus A_S \oplus g_U)$. The result shows that the User Node and the Sensor Node have the same SK.

3.3 A BHDP Design

The BHDP in this paper is based on the existing AODV and makes the Sensor Node confirm all the RREQ/RREP messages of all nodes.

The Sensor Node in the BHDP detects the Black Hole by using the BT in **Fig. 6(a)** and prevents the Black Hole Attack by Broadcasting the detected information to all the nodes within the network. Besides, SK (Session Key) field in **Fig. 6(b,c)** is added to the existing AODV RREQ/RREP message so that the Sensor Node can detect non-authentication node in selecting a message transfer path.

Broadcasting Node	**Source**	**Destination**	**Time Stamp**	**SK**

(a) Broadcasting Table

Type	Flags	Reserved	Hop Count
RREQ(Broadcast)			
Destination IP address			
Destination sequence number			
Source IP address			
Source sequence number			
SK(Session Key)			

(b) RREQ message

Type	A	Reserved	Hop Count
Destination IP address			
Destination sequence number			
Source IP address			
Source sequence number			
SK(Session Key)			

(c) RREP message

Fig. 6. The structure of Broadcasting Table and message

Fig. 7 shows the detection procedure of a Non-Authentication Node and a Black Hole.

The 1st Phase: The source node broadcasts an RREQ message.

The 2nd phase: The Sensor Node confirms the SK of the RREQ message. If the SK of the RREQ message does not exist in the Sensor Node, the Sensor Node decides as a Non-Authentication Node the node that transferred the RREQ message. Then, the Sensor Node informs the Non-Authentication Node and closes the job. If the SK exists in the Sensor Node, go to the 3rd Phase.

The 3rd Phase: The 3rd Phase confirms whether the node that received the RREQ is a Destination Node. If it is a Destination Node, go to the 5th Phase.

The 4th Phase: if it is not a Destination Node, a Node's ID, a Source Address, a Destination Address, Registration Time, and SK value are added to the BT. Then the RREQ Message is broadcast.

The 5th Phase: The Destination Node generates a RREP message.

The 6th Phase: The Destination Node unicasts the RREP message.

The 7th Phase: The Sensor Node confirms the SK of the RREP message. If it does not exist in the Sensor Node, the Sensor Node decides as a Non-Authentication Node the node that transferred the RREP Message. Then, the Sensor Node informs the Non-Authentication Node and closes the job. If the SK exists in the Sensor Node, go to the 8th phase.

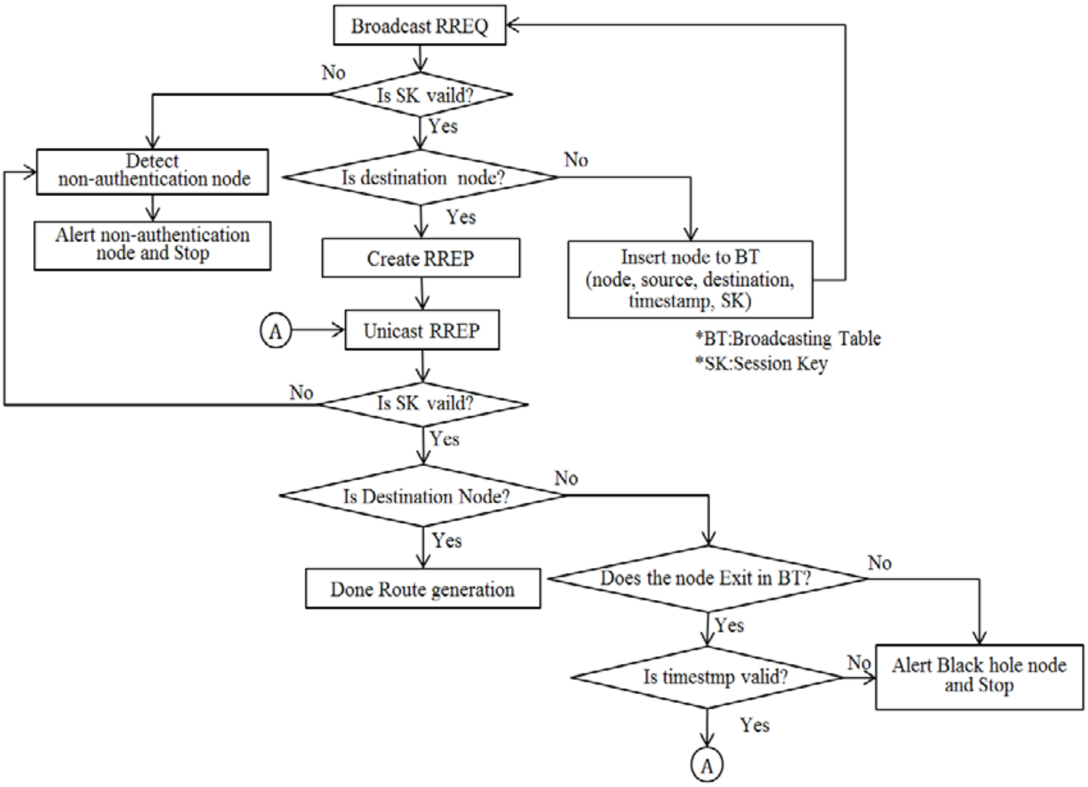


Fig. 7. The detection procedure of a Non-Authentication Node and a Black Hole

The 8th Phase: The 8th Phase confirms whether the node that received the RREP is a Destination Node.

The 9th Phase: If the node that received the RREP is a Destination Node, it confirms that the node that transferred the RREP exists in the BT and the time stamp is valid. If the confirmation is false, the 9th Phase informs that the node which transferred the RREP is a Black Hole and closes the job.

The 10th Phase: If the confirmation is true, the node that received the RREP message unicasts it.

4. Estimation

4.1 The protection of privacy

When the BHDP registers a new vehicle(=user node) to the GWN or requests a Mutual Authentication to the Sensor Node, Eavesdropping Attack or information exposure is likely to happen. But, the MAS can protect a privacy from an eavesdropping attack and an information exposure by hashing a nonce and user's ID and password.

4.2 A Replay Attack

When the BHDP registers a Node to the GWN or requests a mutual authentication to a Sensor Node, a randomly generated nonce and Time stamp are used.

Therefore, although an attacker who intercepted information requests a Node registration and a Mutual Authentication again, the Replay attack can be protected with the nonce and Time stamp.

4.3 A Mutual Authentication Scheme (MAS)

The operation time of the Mutual Authentication in this paper is compared to other schemes with the operation count of hash functions. The result shows that the processing time was improved in **Table 1** more than other schemes.

Table 1. The comparison of computational cost

Authentication	User	Sensor Node	GWN
Proposed scheme	$3T_h$	$3T_h$	$4T_h$
Muhamed et al[19]	$7T_h$	$5T_h$	$7T_h$
Xue et al[20]	$7T_h$	$5T_h$	$13T_h$

T_h : time for a hash operation

Transmission typically consumes more energy than computation because 1 bit transmission is equal to an execution of about 900 CPU instructions [19, 21]. Table 2 shows the comparison of proposed scheme and other related scheme. The propose scheme use four messages for MAS. The result is very similar with Muhamed et al [19] but reduce the number of message than Xue et al [20]. Thus proposed scheme reduce to consume energy than Xue et al [20].

Table 2. The comparison of communication cost

Authentication	The number of message
Proposed scheme	4 messages
Muhamed et al[19]	4 messages
Xue et al[20]	6 messages

4.4 Black Hole Detection Protocol (BHDP)

The BHDP in this paper used an NS-2 [22] Simulator and experimented a simulation with the parameters of **Table 3**. In the experiment, 2 Sensor Nodes, 2 Black Hole, 2 Non-Authentication Nodes and 24 Authentication Nodes were deployed.

Table 3. Simulation Parameters

Parameters	**Values**
Simulation Time	120sec
Simulation Area	1200 × 600m
the number of Authentication Node	24
the number of Sensor Node	2
the number of Black Hole	2
the number of Non- Authentication Node	2
Traffic type	CBR(UDP)
Data Payload	512byte/packet
Transmission Range	200m

The **Fig. 8** shows the location of nodes.

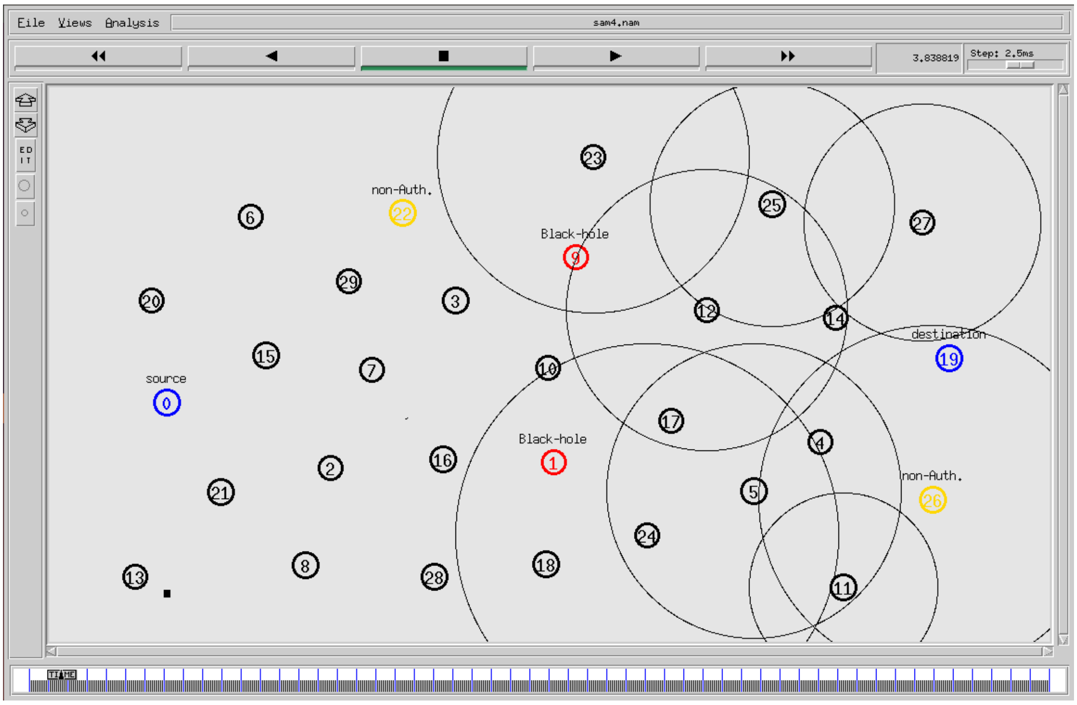


Fig. 8. The location of nodes

Table 4 shows the generated packet, received packet, throughput, packet delivery ratio, and End-to-End delay using formula (1), (2), and (3).

$$\text{Throughput(kbps)} = \frac{\sum Received\ packed}{Stop\ time - start\ time} \times \frac{8}{1000} \tag{1}$$

$$\text{Packet Delivery Ratio(\%)} = \frac{\sum Received\ Packet}{Generated\ Packet} \times 100 \tag{2}$$

$$End - to - End\ Delay(ms) = \frac{\sum(received\ time - send\ time)}{\sum number\ of\ connections} \times 1000 \tag{3}$$

Table 4. The result of simulation (simulation time = 120sec)

	Generated Packet	Received Packet	Throughput (kbps)	Packet Delivery Ratio(%)	End-to-End Delay(ms)
AODV without attack	21,676	4,398	156.87	20.29	219.11
AODV with Black hole (node 1, 9)	21,676	3,391	120.47	15.64	173.06
AODV with Black hole and Non- authentication node (node 1, 9, 22, 26)	21,676	2,849	101.29	13.14	115.28
IDSAODV	21,676	3554	129.12	16.40	136.74
BHDP	21,676	3885	139.57	17.93	146.19

Because the existing AODV generates data transmission paths including a Black hole and non-Authentication node and the Black node and non-Authentication drops the transferred data, data can not be transferred to a destination accurately. The BHDP generates data transmission paths excluding a Black hole and non-Authentication node.

Fig. 9 shows the graph about the comparison result of AODV without Black hole attack, AODV with Black hole and non-Authentication, IDSAODV, and BHDP. Therefore, in the **Fig. 9**, the BHDP which excluded the Black hole and non-Authentication node improves packet delivery ratio more than the AODV(4) and IDSAODV by 4.79% and 1.53% . Also, the BHDP improves Throughput more than the AODV(4) and IDSAODV by 38.28Kbps and 10.45 Kbps.

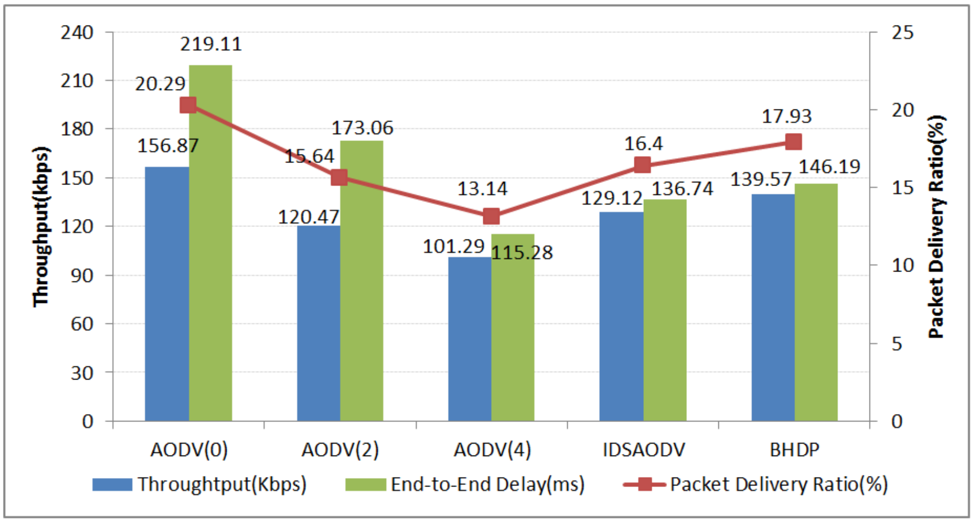


Fig. 9. The result of comparison

Here AODV(0) means AODV without Black hole attack, AODV(2) means AODV with Black hole, AODV(4) means AODV with Black hole and non-Authentication.

5. Conclusions

This paper proposes "A Design of Black Hole Detection Protocol based on a Mutual Authentication Scheme on VANET".

The BHDP has the following characteristics.

First, the computational cost was decreased to average $6T_h$ by reducing the operation count of a hash function more than the existing a Mutual Authentication Scheme.

Second, a privacy was protected from an eavesdropping attack and an information exposure by hashing a randomly generated nonce and user's ID and password.

Third, an replay attack was prevented by using a randomly generated nonce and time stamp.

Fourth, the Black Hole and the Non-Authentication Node was detected by using the SK and BT generated with Mutual Authentication.

Therefore, the BHDP improves Packet Delivery Ratio and Throughput more than the AODV with Black hole and IDSAODV and makes VANET more safe and reliable.

References

[1] S.B. Lee, G. Pan, J.S. Park, M. Gerla, and S. Lu, "Secure incentives for commercial ad dissemination in vehicular networks," in *Proc. of 8th ACM international symposium on Mobile ad hoc networking and computing*, pp.150-159, September 10-14, 2007. Article (CrossRef Link)

[2] S.B. Lee, J.S. Park, M. Gerla, and S. Lu, "Secure Incentives for Commercial Ad Dissemination in Vehicular Networks," *IEEE Transactions on Vehicular Technology*, vol.61 no.6, pp.2715-2728, July, 2012. Article (CrossRef Link)

[3] H. Hartenstein and L.P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Communication magazine*, vol.46, no.6, pp.164-171, June, 2008. Article (CrossRef Link)

[4] Y. Toor, P. Muhlethaler and A. Laouiti, "Vehicle ad hoc networks: applications and related technical issues," *IEEE communications surveys & tutorials* vol.10 no.3, pp.74–88, September, 2008. Article (CrossRef Link)

[5] Hsin-Te Wu and Wen-Shyong Hsieh, "RSU-based message authentication for vehicular ad-hoc networks," *Multimedia Tools and Applications*, vol. 66, no.2, pp.215-227, September, 2013. Article (CrossRef Link)

[6] Aijaz, A., Bochow, B., Florian, D., Festag, A., Gerlach, M., and Kroh, R., "Tim Attacks on Inter Vehicle Communication Systems - an Analysis." in *Proc. of 3rd WIT*, pp.189-194, 2006. Article (CrossRef Link)

[7] K. Plossl, T. Nowey and C. Mletzko, "Towards a security architecture for vehicular ad hoc networks," in *Proc. of 1st International Conference on Availability, Reliability and Security (ARES2006)*, pp.374-381, April 20-22, 2006. Article (CrossRef Link)

[8] C.E. Perkins and E.M. Royer, "Ad-Hoc On-Demand Distance Vector Routing," in *Proc. of 2nd IEEE Mobile Computer Systems and Applications*, pp. 90–100, February 25-26, 1999. Article (CrossRef Link)

[9] C. Perkins, E. Beliding-Royer and S. Das, "Ad hoc on-demand distance vector (AODV) routing," *ietf internet draft*, 2003, Article (CrossRef Link)

[10] Watchara Saetang and Sakuna Charoenpanyasak, "CAODV Free Blackhole Attack in Ad Hoc Networks," in *Proc. of 2012 International Conference on Computer Networks and Communication Systems (CNCS 2012), IPCSIT* vol.35, pp.63-68, 2012. Article (CrossRef Link)

[11] Luke Klein-Berndt, "A Quick Guide to AODV Routing," Article (CrossRef Link)

[12] Nital Mistry, Devesh C Jinwala, ans Mukesh Zaveri, "Improving AODV Protocol against Blackhole Attacks," in *Proc. of the International Multi Conference of Engineers and Computer Scientists 2010, IMCES 2010*, vol.2, pp.1034-1039, March 17-19, 2010. Article (CrossRef Link)
[13] L. Raja and S. Santhosh Baboo, "Analysis of Blackhole attacks on AODV Routing Protocol in MANET," *IJCSET*, vol. 2, no. 12, pp.1522-1526, December, 2012. Article (CrossRef Link)
[14] Ming-Yang Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems," *Computer Communications*, vol.34, no.1 pp.107–117, January, 2011. Article (CrossRef Link)
[15] S. DOKURER, "Simulation of Black hole attack in wireless Ad-hoc network," *Master's thesis Atılım University*, September 2006. Article (CrossRef Link)
[16] Samah Ahmed Senbel, Ahmed Ibrahim and Nagy E Zaki, "Solution to Black Hole Attack in Ad Hoc on Demand Distance Vector Routing Protocol," *Journal of Computer Sciences and Applications*, vol. 3, no. 4, pp.90-93, 2015. Article (CrossRef Link)
[17] Ankita Chaturvedi and Sanjiv Sharma, "A new Technique for Preventing Black Hole Attack in Mobile Ad-hoc Network," *International Journal of Advance in Computer Science and Technology*, vol 3, No. 10, October 2014. Article (CrossRef Link)
[18] P.N. Raj and P.B. Swadas, "DPRAODV a dynamic learning system against blackhole attack in aodv based manet," *International Journal of Computer Science Issue*, vol. 2, pp. 54-59, 2009. Article (CrossRef Link)
[19] Muhamed Turkanović, Boštjan Brumen, and Karko Hŏlbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," *Ad Hoc Networks*, vol. 20, pp.96-112. September, 2014. Article (CrossRef Link)
[20] K. Xue, C. Ma, P. Hong and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," *Journal of Network and Computer Applications*, vol.36, no.1, pp.313-323, January 2013. Article (CrossRef Link)
[21] C.C. Chang, D.J. Nagel, S. Muftic, "Assessment of Energy Consumption in Wireless Sensor Network: A Case Study for Security Algorithm," *Mobile Adhoc and Sensor Systems, 2007. MASS 2007 IEEE International Conference on*, pp.1-6, October 8-11, 2007. Article (CrossRef Link)
[22] NS-2 Simulator, Article (CrossRef Link)

ByungKwan Lee received his B.S. degree from Pusan National University in 1979, the M.S. degree in Computer Science from Chung-Ang University in 1986 and the ph.D. degree in Computer Science from Chung-Ang University in 1990 in Korea. He has been a professor of Computer Science at Catholic Kwandong University in Korea since 1988. He was a visiting professor at Saginaw Valley State university, Michigan, USA during 2000~ 2001. He is a permanent member of the KISS and KIPS. His current research interests are network security, Wireless Sensor Network Security, Internet of Things and Big Data.

EunHee Jeong received her B.S. degree from Kangneung National University in 1991, the M.S. degree in Computer Science from Kwandong University in 1998 and the Ph.D. degree in Computer Science from Kwandong University in 2003 in Korea. She has been a professor of department of Regional Economics at Kangwon National University in Korea since 2003, Sept. She is a regular member of the KSII. Her current research interests are Sensor Network, IT security, web programming, and e-commerce security.