An Efficient Detection And Management Of False Accusation Attacks In Hierarchical Ad-Hoc Networks

Yunho Lee[1], Sang-Guun Yoo[2] and Soojin Lee[1]
[1] Department of Defense Information Science, Korea National Defense University
Seoul, Republic of Korea
[2] Department of Computer Science and Engineering, Sogang University
Seoul, Republic of Korea
[e-mail: {yunholee, cyberkma, sangguun}@gmail.com]
*Corresponding author: Yunho Lee

Received May 18, 2011; revised March 22, 2012; revised June 14, 2012; accepted June 20, 2012; published July 25, 2012

Abstract

An approach to detect abnormal activities based on reputations created individually by each node is vulnerable to a false accusation since intrusion detection in ad-hoc networks is done in a distributed and cooperative manner. Detection of false accusation is considered important because the efficiency or survivability of the network can be degraded severely if normal nodes were excluded from the network by being considered as abnormal ones in the intrusion detection process. In this paper, we propose an improved reputation-based intrusion detection technique to efficiently detect and manage false accusations in ad-hoc networks. Additionally, we execute simulations of the proposed technique to analyze its performance and feasibility to be implemented in a real environment.

Keywords: Ad-hoc network, intrusion detection, false accusation, reputation

http://dx.doi.org/10.3837/tiis.2012.07.009

1. Introduction

Since ad-hoc networks allow a network to be configured quickly and to keep it operational without infrastructure, they could be applied in a variety of areas such as military tactical situations, emergency disaster situations, the establishment of temporary conferences, and so forth. It has been known, however, that they may be vulnerable regarding security, and also that it may be difficult to implement security measures because of their specific properties which differ from existing networks. In addition, most protocols applied to ad-hoc networks are subject to cooperation between each node, so that the efficiency of whole networks is severely degraded even by the simple malicious activities of a few nodes. This could be well confirmed in the result of the simulation based study presented by [1].

As a result of these issues many approaches were proposed. One of the first one was [2], which proposes the premise of a distributed and cooperative structure as the fundamental concept for intrusion detection in ad-hoc networks; this idea has been applied in many subsequent studies. In carrying out intrusion detections, one method which was proposed is that each node participating in the network continuously monitors the activities of neighborhood nodes, and a certain node is regarded as an intruder node if it continues to perform malicious activities at a greater level than a pre-defined threshold [3]. Another method which was also proposed is that a reputation score is determined for a certain node with weights, and the scores which are evaluated independently by each node are aggregated to determine whether or not malicious activities of a certain node [4][5][6].

However, these approaches, which detect malicious nodes to exclude them with reputation scores in ad-hoc networks, are vulnerable to false accusations [7][8]. In the process in which neighborhood nodes exchange reputation scores of a certain node in order to aggregate a reputation for the corresponding node, some nodes may conspire together to signify a normal node as an intruder node or compromised nodes may report the wrong reputation scores to neighborhood node. In these cases, normal nodes are excluded from the routing process which means that the overall efficiency of the network could be also degraded. Therefore, in order to detect and respond to malicious activities by using reputations in intrusion detection with a distributed and cooperative structure as a premise, it is essential to use a technique to minimize the negative effects of false accusations.

In this paper, we propose a reputation-based intrusion detection system for multi-layered ad hoc networks that incorporates a technique to detect and manage false accusations. The proposed solution configures the upper layer nodes as NWMS (Node Weight Management Server) nodes to comprehensively manage the weights for nodes making false accusations and to ensure more reliable reputation management. In addition, for nodes that unfair weights are assigned due to temporary network failures, their survivability is increased through a compensation algorithm. On the other hand, the ElGamal cryptography, which is based on the difficulties of solving discrete algebraic problems, was applied to solve the false accusation problem by collusion.

The rest of the paper is organized as follows. Section 2 briefly reviews some intrusion detection techniques used to detect and manage abnormal activities in the ad-hoc networks, and analyzes their limitations. Later in section 3, we describe the proposed detection and management technique for malicious nodes making false accusations. Then, the section 4

describes the analysis results of simulations of the proposed solution performed using NS-2. Finally, section 5 concludes the paper.

2. Related Work

Research related with detection and management of misbehaving nodes in ad-hoc networks have been developed for many years. One of the first researches related with intrusion detection structures and techniques was proposed by Zhang et al. [2]. This research proposes a premise of distributed and cooperative structure to detect intrusions, and this idea has been used by many other subsequent studies. One of the first important approaches in intrusion detections were proposed by Mart et al. in [3] called the 'Watchdog' technique. This approach includes a watchdog module in which every node in the network can monitor neighborhood nodes to detect misbehaving nodes; the pathrater, which is another module, helps find the best path which avoids misbehaving nodes based on the detection results of the watchdog.

The CONFIDANT(Cooperative Of Nodes, Fairness In Dynamic Ad-hoc NeTworks) [4][5] protocol, which was proposed as an extended technique of Watchdog and pathrater, includes a method for excluding misbehaving nodes from the network by isolating them. The CONFIDANT protocol is composed of modules such as monitor, reliability manager, evaluation system, and path manager. The monitor module plays a role to detect abnormal activities in neighborhood nodes, and the reliability manager module takes charge of transferring alarm messages generated when detecting abnormal activities. The evaluation system module manages a list of malicious nodes by managing classes for nodes with a scheme similar to one used in an online auction system, and gradually exchanges it for nodes having friendly relations. The path manager module re-ranks path according to security metrics, e.g., reputation of the nodes in the path, and deletes paths containing misbehaving nodes.

Additional to Watchdog and CONFIDANT, many other approaches have been proposed for intrusion detection. In [9], Tseng et al. propose a specification based intrusion detection model for the OLSR ad-hoc routing protocol; in this solution, they define specifications of mandatory conditions for control messages used in the path establishment and those specifications are used to detect intrusions. Mitrokosa et al. propose an anomaly detection technique to detect new forms of attacks such as selective packet drop in [10]; this technique is based on a neural network and evaluates for packet dropping attacks using features selected from the MAC layer. In [11], Gonzalez et al. propose a mechanism to detect black hole (which does not forward any packet) and gray hole (which only forwards selectively some packets) attacks by using learned statistical values of transmitted and received packets. Sen et al. proposes in [12] proposes a method to detect selfish nodes by using finite state machine that watch over the normal forwarding of RREQ(Route REQuest) messages transmitted by nodes in the path establishment stage. For additional information of other approaches, we recommend to read [13].

All the mentioned solutions propose interesting solutions to misbehavior detections. However, they rely on the specification of normal behavior or dissemination of information of observed behavior making them vulnerable to false accusations, which can seriously degrade the performance and jeopardize the functionality of network. To demonstrate the gravity of the false accusation in the performance of the network, we have simulated the AODV (Ad-hoc On-demand Distance Vector) protocol with the two types of misbehaving nodes classified by Gokhole et al. in [14]. They classify the misbehaving nodes in selfish and malicious nodes. A

selfish node only transmits/forwards their packets and avoids the forwarding packets of other nodes to save their resources and energy; on the other hand, malicious nodes, whose goal is to isolate the network and energy depletion of neighbor nodes, executes attacks such as fabrication, modification, blackhole, wormhole attacks. Inside the fabrication attack we can include the false accusation which fabricates false alert messages accusing normal nodes as misbehaving nodes. The simulation was executed using the AODV protocol with 10% of selfish nodes and 10% of false accusation nodes (see **Fig. 1**); the result of the simulation shows how false accusation attack produces a fast throughput reduction over the time demonstrating that the false accusation node can affect more dramatically than the selfish nodes.

We can summarize the limitation of the existing works as follows. First, most studies do not consider a response method for false accusations that a certain node reports normal nodes as misbehaving nodes for a malicious purpose. Second, if the nodes perform abnormal activities intelligently maintaining misbehaviours below to the predefined threshold, the attack would not be alerted, allowing the abnormal activities to continue. Third, even for nodes working normally, they may be isolated or excluded from the network because their evaluated reputation score reaches the threshold. In the detection method for abnormal activities, these nodes may be reported as misbehaving nodes due to communication failures caused by instantaneous errors or detection failures caused by communication collisions, although they work normally. For all these reasons, this paper presents an improved reputation-based detection and management method for nodes with abnormal activities in order to solve the mentioned limitations of the existing works.

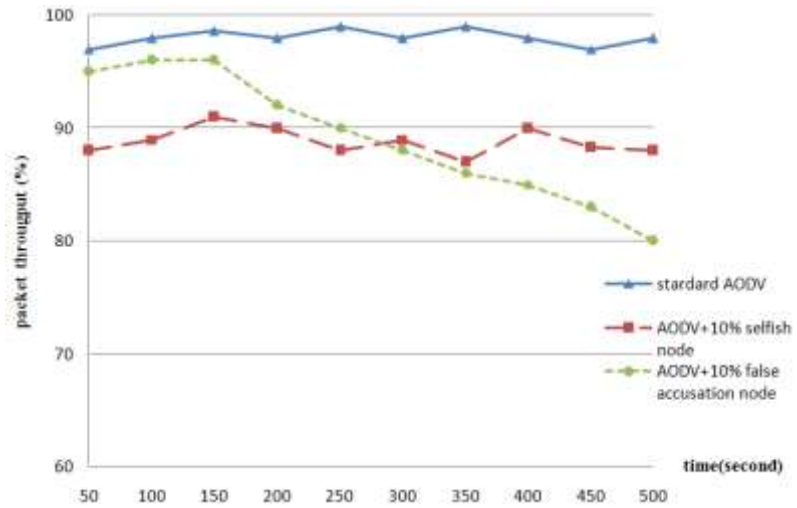

Fig. 1. Analysis of influence of 'selfish nodes' and 'malicious nodes executing false accusations' in the network performance

3. Reputation-based Intrusion Detection Technique

3.1 Assumption

In this paper, we propose a reputation-based intrusion detection technique for multi-layered ad-hoc networks. To apply the technique proposed in this paper, the working environment of each node is assumed as follows. First, the network model uses the tactical ad-hoc network [15][16][17][18][19][20][21], which is actively being studied in many countries, including in

the United States. Contrary to general ad-hoc networks, the tactical ad-hoc network forms a hierarchical structure where the upper layer nodes are considered secure and have sufficient energy and stability. **Fig. 2** illustrates the structure of a common tactical ad-hoc network. Second, every node in the network operates in 'promiscuous mode' to be able to overhear transmissions of neighboring nodes located within the transmission range. Each node uses an omni-directional antenna to transmit their packets; therefore, neighbor nodes generate an overlapped communication range between them (see **Fig. 3**). Third, each node has its own private key, and an upper layer node has the private keys of all the nodes.

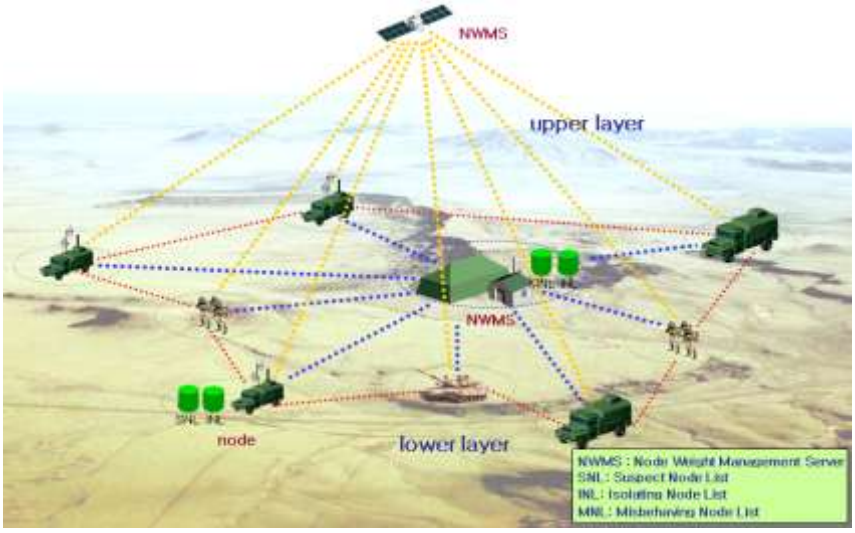

Fig. 2. The structure of tactical ad-hoc network

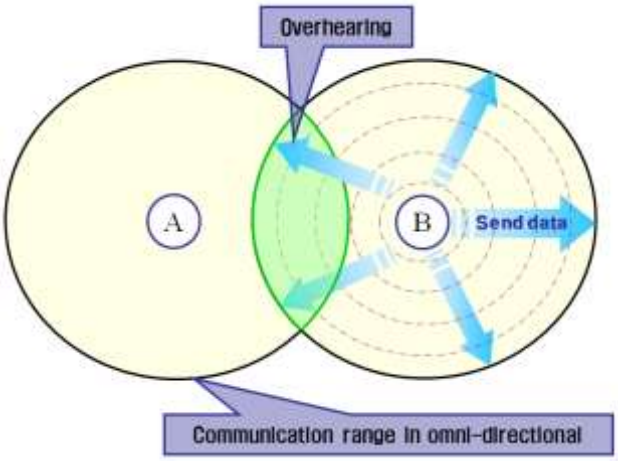

Fig. 3. Overhearing method

3.2 Attack model

Since most routing protocols for ad-hoc networks studied until now do not consider malicious false accusations, if a node with abnormal activities accuses a normal node as a malicious node, the normal node may be excluded in the routing setup stage to isolate it from the network. Therefore, the routing protocol, which considers the safety of the ad-hoc network and also

ensures the best possible performance, should consider detection and exclusion of malicious nodes making false accusations as well as for nodes with usual abnormal activities. This paper models an attack with an abnormal activity as a node which does not forward packets for a certain time, and a model of the malicious false accusation attack, which is defined as follows.

As shown in **Fig. 4**, to isolate node C on the path from the network, the malicious node B reports to the source node S falsely as node C did not deliver data sent to the destination node D by node S, although node C normally delivers the data. At this time, the destination node D sends an ACK (Acknowledgement) message because it received the data normally. However, the malicious node B does not send and discards the ACK message in order to conceal its own action. If the source node S does not receive the ACK message from the destination node for a certain time, it mistakes node C for the node with abnormal activities based on node B's report to propagate this fact to neighboring nodes, and as a result, the normal node C may be excluded from the network.

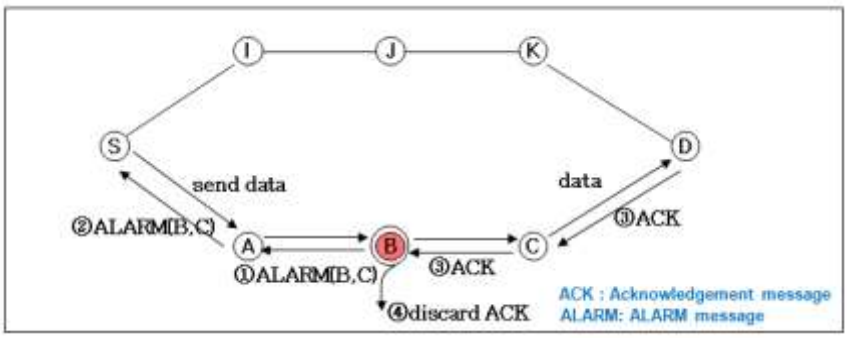

Fig. 4. Example of a false accusation

3.3 Intrusion detection algorithm

In order to solve the false accusation problem in ad-hoc networks, the routing protocol proposed in this paper is designed by modifying the existing AODV protocol [22] enabling it to effectively detect false accusations but to minimize the additional communication overhead.

3.3.1 Use of terms

Communication messages used in the proposed intrusion detection technique and tables managed additionally in each node are as follows. First, the message used in the path finding stage adds two fields for confirming the path into the RREQ and RREP packets of the AODV. The *Route* field is a value sequentially connecting the unique IDs of nodes passed through by the RREQ and RREP packets. The *Route_verifi_val* field is to check the accuracy of paths passed through by the RREQ and RREP packets, which is a value accumulating each node's private key to multiply exponentially ($g^{k_a} \bmod p$: g, p are public values and k_a is node A's private key).

- RREQ(Src_addr, Brd_id, Dest_addr, Dest_seq_#, hop_cnt, *Route*, *Route_verifi_val*)
- RREP(Src_addr, Dest_addr, Dest_seq_#, hop_cnt, life_time, *Route*, *Route_verifi_val*)

If each node identifies a misbehaving node by overhearing whether or not the neighboring nodes on the path transfer data normally, then the node reports it to the source node with an ALARM message, and the message format is as follows. The *Notify_node_addr* and the *Misbehaving_node_addr* variables mean a reporting node and a node with abnormal activities, respectively.

■ ALARM(*Notify_node_addr, Misbehaving_node_addr*)

If the destination node repeatedly receives the same data from the source node together with an ALARM message within a certain time, it identifies the node reporting the ALARM message as the malicious node and notifies it to the source node. The format of the NWARN (Node Warning) message used at this time is as follows, and this message is also used when the source and destination nodes notify the corresponding node to the NWMS.

■ NWARN(Notify_node_addr, Malicious_node_addr, *Route*, *Route_verifi_val*)

If a node on the path receives the NWARN message, it registers the malicious node in the message in its own SNL(suspect node list) to manage it, and its format is as in the table below, in which the count value is set as 1 initially, and can go up to 5. In addition, if each node receives the nodes to be isolated from the NWMS, it registers them in its INL(isolating node list), and its format is as in **Table 1**.

If the NWMS receives information on misbehaving nodes from the source and destination nodes respectively, it registers the corresponding nodes in its MNL(misbehaving node list) to manage the weight; its format is as the in following **Table 2**, in which the weight is set as 1 initially, and can go up to 5.

Let's consider an example. Consider the **Fig. 4** where a malicious node B with node ID equal to NID_0002 executes misbehaviors. When a misbehaving activity of the node B is detected by the node A, this node creates a row in its SNL with sequence number=1, node ID=NID_0002, and count=1 as shown in **Table 1**. The sequence number and count are equal to 1 because it is the first row created in the table and it is the first time the misbehavior of the node B is detected. On the other hand, when the NWMS receives information about the misbehaving node B from the source and destination nodes respectively, the NWMS creates a row in its MNL including the sequence number=1, node ID=NID_0002, and weight=1 as shown in **Table 2**. If the misbehaving activity of the node B were detected more than 5 times by the node A, or if the node A receives a message from the NWMS saying that the node B is an isolated node, it would register the node B in its INL as shown in **Table 1**.

Table 1. SNL and INL

sequence number	node ID	count
1	NID_0002	1

sequence number	node ID
1	NID_0002

Table 2. MNL

sequence number	node ID	weight
1	NID_0002	1

3.3.2 Establishment of Multiple Paths

This paper uses a scheme to establish multiple paths for rapid retransmission in case of packet transfer failure or communication disruption caused by malicious nodes on the path. For the traditional scheme to set multiple paths, the source node broadcasts the RREQ message in the initial stage to find the routing path, this message then arrives at the destination node through several nodes, and the destination node retransmits the RREP message. At this time, the destination node can establish multiple paths by sending several RREP messages to the neighboring nodes in ascending order of the number of hops from the RREQ messages which arrive within a certain time.

The proposed protocol in this paper improves the AODV protocol for selecting the optimum routing path. If the destination node receives the RREQ message, it considers not only the count value of the corresponding node together with whether or not the intermediate nodes on the path included in the RREQ are contained in its own SNL table but also the number of hops of the corresponding paths. The equation used for selecting the optimum path is as follows, and it selects up to the third path in ascending order of the *PT(Path Trust)* value found by this equation. The meaning of $\sum N_{count} * 0.2$ in this equation is that the PT value is increased by '1' if nodes in the entry path are included in own SNL table, and the number of nodes that its count(N_{count}) corresponds to the maximum value is more than one.

$$PT = hop_{count} + \sum N_{count} * 0.2 \tag{1}$$

In other words, our proposal includes another variable to the AODV routing protocol for the best routing path selection. The equation (1) helps to find more reliable routing path considering both the distance (using hop_{count}) and trustiness (using N_{count}, the reputation of nodes).

3.3.3 Detection of Nodes Making False Accusation

Fig. 5 is the scheme proposed to effectively detect the malicious nodes making false accusations examined in the definition of the attack model in section 3.2.

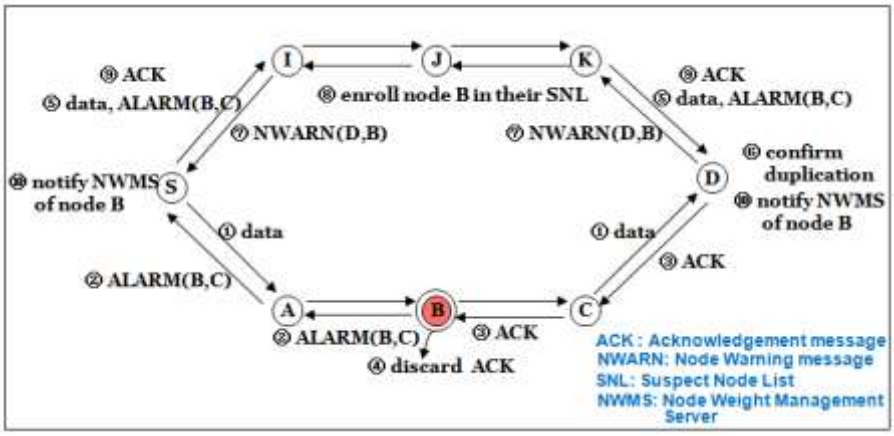

Fig. 5. Detection procedure of false accusations

A situation is assumed in which a malicious node B on the path accuses a normal node C falsely when a source node S transfers data to a destination node D. That is, the malicious node B falsely sends an alarm(B, C) message to the source node S as the normal node C did not deliver data. If the source node does not receive an ACK message from the destination node

within a certain time, it retransmits the data and the alarm(B, C) message via the second best path. At this time, if the destination node repeatedly receives the same data from the same source node within a certain time, it could determine the reporter of the corresponding alarm message (in this case the node B) to be the malicious node, accusing the false suspect. It has used the fact that a data packet could not be repeatedly received because it is a unicast packet. The destination node D sends a NWARN(D, B) message to notify the source node S about the malicious false accusation of the node B. The detailed operating procedure of intermediate nodes receiving this message is as shown in **Fig. 6**.

First, the intermediate node checks whether or not the malicious node is included in the received NWARN message which already exists in its own SNL, and if it does not exist, it newly registers to assign the count value as 1, or if it does exist, it increases its value by 1 (the maximum value is 5). If the source node S receives a NWARN(D, B) message, it sends an ACK message to the destination node to notify that it received it normally, and the source and destination nodes report node B to the NWMS. Like this, the decision of whether or not a node has abnormal activities is carried out by cooperation of the source and destination nodes. The details of the detection algorithm is explained in **Fig. 7**.

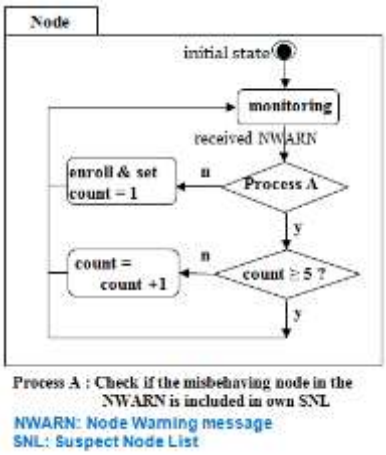

Fig. 6. Procedure steps when intermediate nodes receive a NWARN message

Fig. 8 shows the operating procedure of the NWMS received information regarding the suspicious node from the source and destination nodes. The NWMS receives the report and compares two reports which arrive within a certain time, and it decides whether or not the suspicious nodes are identical. If they are the same information, it checks whether or not the suspicious node is the one already registered in its own MNL, and increases the weight value by 1. If the weight exceeds the threshold, the NWMS broadcasts it to every node, and each node which receives this message deletes the corresponding node from its own SNL, and it registers the corresponding node to the INL to exclude it from the routing process.

Proposed Misbehaving Node Detection Algorithm
Detect Selfish Node **1.** Overhear a transmission signal of the neighbor node **2.** *if* (not hear for a certain time) // not forwarding packets **3.** Send ALARM message to the source node

```
Detect Malicious Node
1. if(receive ALARM message)
2. Compare the current received data packet
        with the set of previously received data packets
                //check multiple copies of the same data
3. if(confirm duplication reception)
4.   determine the reporter as the false accusation node
5. else
6.   determine the accused node as the selfish node
```

Fig. 7. Proposed misbehaving node detection algorithm

3.3.4 Detection of Collusive Nodes

In the proposed routing protocol, the source and destination nodes report nodes with false accusations to the NWMS, which is an upper layer' node. However, two malicious nodes in the network could collude to falsely report a certain node. To solve such a problem of collusive nodes, this paper uses a solution applying the ElGamal cryptography based on the difficulties of discrete algebraic problems. In other words, it uses a fact that g and p are the public values in the equation $y_a = g^{k_a} \bmod p$, and if k_a is given, y_a is easily known, but the reverse is extremely difficult.

Each node received the RREQ message in the path finding stage adds its own address information into the Route field and exponentially multiplies the *Route_verifi_val* field with its own private key to send it. In other words, if the node A receives the RREQ message from the source node S as shown in Fig. 3, the Route field of the RREQ becomes as S-A, and the *Route_verifi_val* field becomes as $g^{k_s k_a} \bmod p$. If the source and destination nodes receive the RREQ and RREP messages by such a scheme, the address chain and path identification values of the corresponding path could be obtained. If the source and destination nodes identify the malicious node, they would notify this value with the NWARN message to the NWMS. Since the NWMS has private keys for the whole nodes, it could compare the path identification value with the address chain to identify the false report action by collusion of two nodes.

3.3.5 Relief of Nodes Receiving Unfair Weights

If an unfair weight is assigned to a normal node due to errors in communication, etc., a relief method is needed for this. This paper has a relief scheme to reduce the unfair weight for nodes participating in the transmission of normal packets. **Fig. 9** shows the operating procedure to relieve a node if detecting normal operations of a neighboring node registered in its own SNL. In other words, if a node included in its own SNL sends packets normally, it decreases the count value by 1, and reports the node to the NWMS. The NWMS checks the weight of the corresponding node, and if it is not 0, it decreases 0.1, or if the weight becomes 0, it broadcast this to all the nodes to make them delete the corresponding node from the SNL.

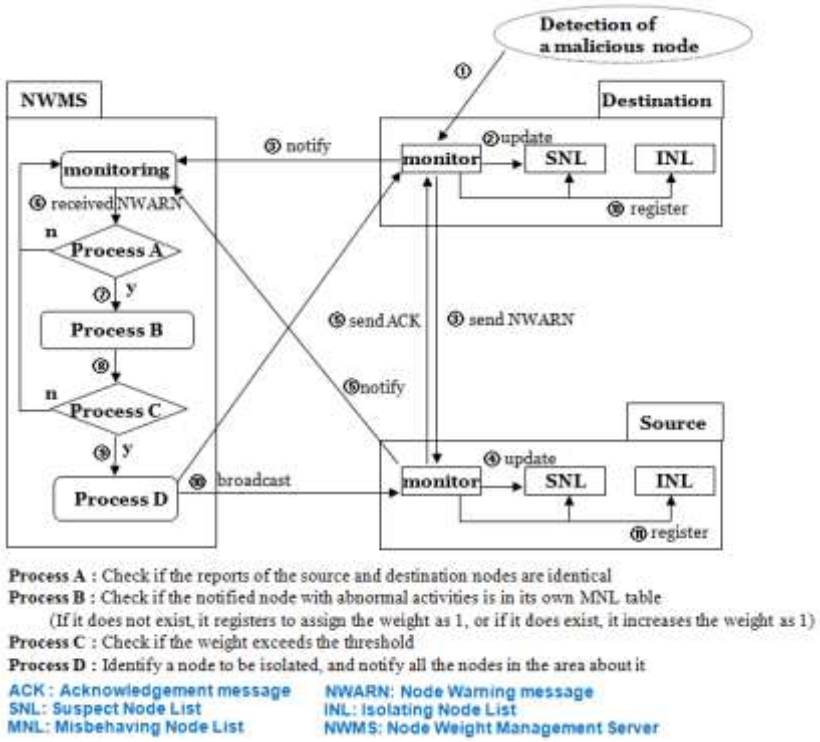

Fig. 8. Procedure steps of the NWMS

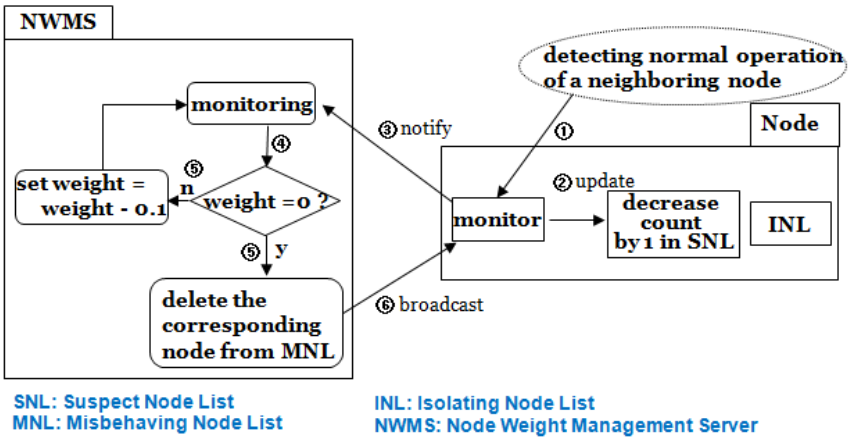

Fig. 9. Rescue procedure of a normal node

4. Performance Evaluation

We evaluate the performance of the proposed technique and compare with existing approaches. The evaluation was carried out in simulation as well as mathematical analysis scheme.

4.1 Experimental Environment And Its Scenario

We simulated the proposed technique on NS-2 and compared with the existing secure ad-hoc routing protocol such as Watchdog and CONFIDANT. The experiment mainly measured the

packet throughput depending on the variation of the number of nodes with abnormal activities and the performance of the detection and exclusion of nodes with abnormal activities. Analysis on the routing overhead used a mathematical analysis scheme. The setting values for the simulation are given in **Table 3**.

In the experiment, we have separated two types of misbehaving nodes. The first type of misbehaving nodes correspond to the selfish nodes which do not forward the received packets and the second type of misbehaving nodes correspond to the malicious nodes which makes false accusations. The ratio of each type of misbehaving nodes correspond to the 50% of the total of misbehaving nodes. The ratio of misbehaving nodes in simulations was increased to be 10%, 20%, and 30% of the total number of nodes. Simulation with higher number of misbehaving nodes was not executed because we have considered such condition would be unrealistic. We have set a high ratio of misbehaving nodes because the tactical ad-hoc networks have more probabilities for trusted nodes being compromised and then being used by adversary to launch attacks on networks [19].

In addition, the simulation environment was designed to process the report and notification control packet as a unicast packet for decreasing communication overhead. The value of 1 as the increase rate of MNL's weight, 5 as the threshold, 1 as the increase rate of SNL's count value, 1 as the decrease rate, and 5 as the maximum value were set in this experiment. The reason why the threshold was taken as 5 is explained in section 5.

Table 3. Simulation parameters

Parameter	Level
Area	1000m x 1000m
Simulation time	1000sec
Packet generation interval	100ms
Packet size	64 byte
Number of nodes	500
Speed	0 ~ 5m/s
Threshold	5
Radio Range	200m
Ratio of the number of nodes with abnormal activity	10, 20, 30%

4.2 Results of the experiment

4.2.1 Network Throughput Depending On The Variation Of The Number Of Nodes With Abnormal Activities

Fig. 10, Fig. 11, Fig. 12 show network throughput of the Watchdog, CONFIDANT and the proposed technique as the percent of nodes with abnormal activities is increased to be 10%, 20%, and 30% in the network, respectively. Of course, the number of nodes which make false accusations also simultaneously increase because the ratio of malicious nodes with false accusation occupies 50% of the nodes with abnormal activities. Since the period of generating traffic is 100ms, the maximum number of packets generated every 100 seconds is 1000, and the amount of processing packets is aggregated in a 100 second unit. Analyzing the results of the experiment comprehensively, the proposed technique shows the best performance because it could not only quickly retransmit data by establishing the optimum reliable multiple paths even if the number of nodes with abnormal activities is increased in the network, but it could

also detect the malicious nodes with false accusations as well as the nodes simply discarding packets as time passes in order to exclude them from the network.

The Watchdog protocol has a simple function that identifies nodes with abnormal activities of discarding packets and avoids them. Therefore, network throughput is decreased as the ratio of including nodes with abnormal activities is increased, however, it could ensure constant network throughput because it is not affected by malicious nodes with false accusations. On the contrary, although the detection algorithm of CONFIDANT protocol could detect nodes with abnormal activities to exclude them from the network, it does not in the least consider the malicious nodes with false accusations. As shown in the results of experiment, although the CONFIDANT protocol improves the performance a little in the initial stage by detecting the nodes with abnormal activities to exclude them, it shows a rapid degradation effect in performance due to the exclusion of normal nodes from the network because it is affected by the malicious nodes with false accusations as time passes. In other words, although it could suitably detect and exclude nodes with simple abnormal activities, it is fatally damaged due to malicious false accusations.

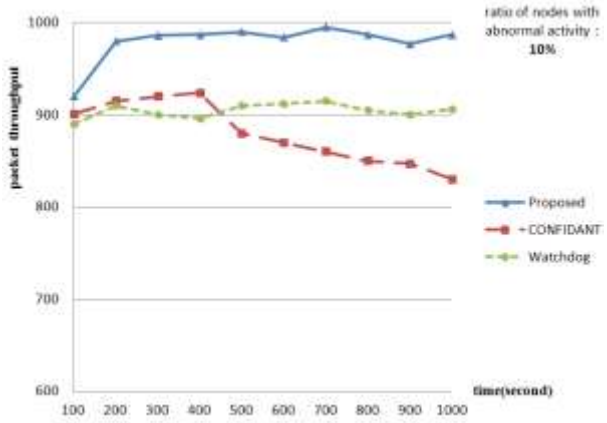

Fig. 10. Packet throughput in the cases where the ratio of nodes with abnormal activity is 10%

As examined in the results of the experiment, it could be said that consideration of malicious false accusations is surely essential in the design of an algorithm to detect the nodes with abnormal activities in the ad-hoc networks.

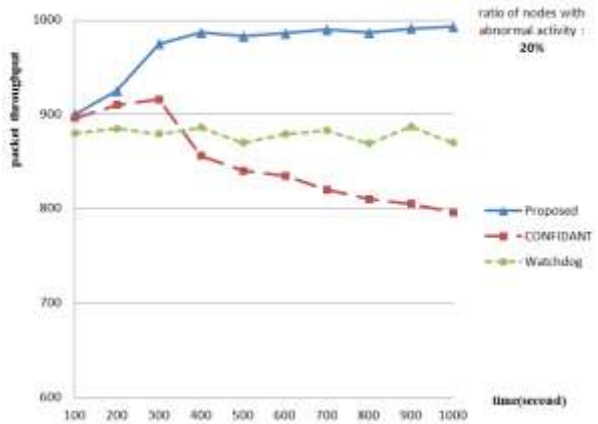

Fig. 11. Packet throughput in the cases where the ratio of nodes with abnormal activity is 20%

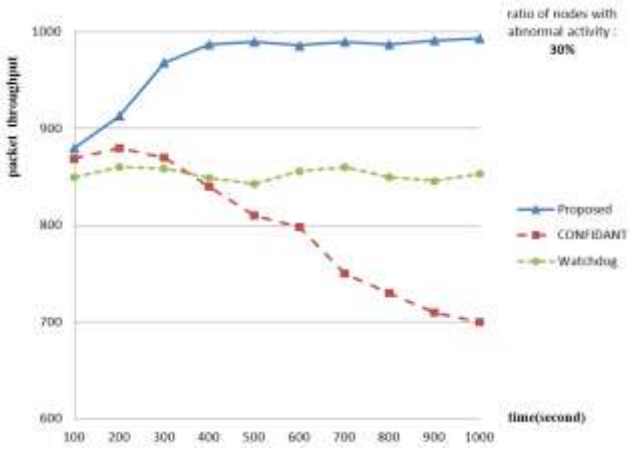

Fig. 12. Packet throughput in the cases where the ratio of nodes with abnormal activity is 30%

4.2.2 Detection and Exclusion Performance Of The Nodes With Abnormal Activities

Fig. 13 compares the detection and exclusion performance for the nodes with abnormal activities in the network. The scheme proposed in this paper could detect not only the nodes simply discarding packets but also the malicious nodes with false accusations.

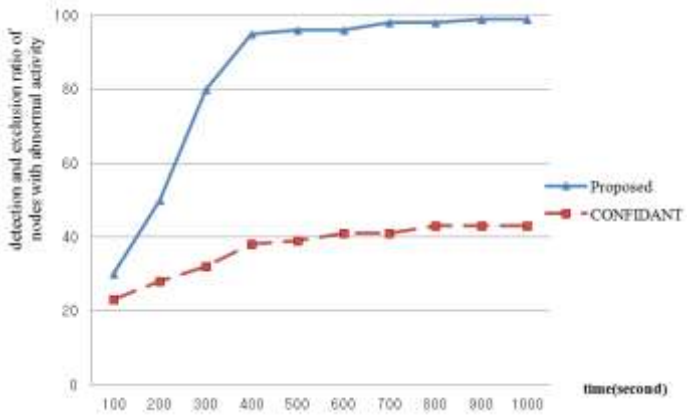

Fig. 13. Detection and exclusion performance of the nodes with abnormal activities

In addition, it shows the best performance because it could continuously manages the nodes with abnormal activities through the NWMS even if they move. On the contrary, the CONFIDANT protocol shows a little lower performance because it could not detect the malicious nodes with false accusations, and the method to detect the node with abnormal activities discarding packets shares information only between neighboring nodes on the routing path so that it is difficult to detect if they move to other locations without exceeding the threshold. Although the Watchdog has the algorithm to detect the nodes with abnormal activities, it is excepted as a the target of comparison in this experiment because it does not include the algorithm to exclude them.

4.2.3 Routing Overhead Analysis

In this section, we provide an analysis of the routing communication overhead in terms of

mathematical and experimental analysis.

The communication overhead is increased a little in the case of applying the proposed method compared to the existing routing protocol. The reason is that the control packets are generated for detecting and managing the nodes with abnormal activities. Packets additionally generated are the NWARN packet with which the destination node reports the malicious nodes with false accusations to the source node as a unicast, the ACK packet with which the source node informs the normal receiving of the NWARN packet to the destination node, the NWARN packet with which the source and destination nodes report the malicious nodes to the NWMS, and the packet that the NWMS broadcasts to all the nodes in the area. The equations to estimate the communication overhead generated by nodes to report abnormal activities are Eq. (2), (3), (4), and (5).

If the number of generating packets per second is $\boldsymbol{t}$, the average number of nodes including the routing path is $\boldsymbol{p}$, the packet size is $\boldsymbol{NP_{size}}$, the total number of nodes is $\boldsymbol{N}$, the number of nodes with abnormal activities is M, the average occurrence number of abnormal activities during the whole experimental time is r, the size of report and control packets is CP_{size}, the time of the simulation is T, and the average number of nodes included on the path from the reporting node to the NWMS is n, then the overhead V for transmitting the NWARN packets and the acknowledged ACK packets between the source and destination nodes is as given in Eq. 2,

$$V = p * CP_{size} * M * r * 2 \tag{2}$$

the overhead U generated when the source and destination nodes report the suspicious nodes to the NWMS is as in Eq. 3,

$$U = n * CP_{size} * M * r * 2 \tag{3}$$

the overhead B generated when the NWMS broadcasts the nodes with abnormal activities is as in Eq. 4,

$$B = M * CP_{size} * N \tag{4}$$

and the overhead O compared to the total communication traffic generated during the experimental time could be expressed as in Eq. 5,

$$O = \frac{V * U * B}{T * t * p * NP_{size}} \tag{5}$$

Additional to the mathematical analysis of the routing communication overhead, we have performed simulations to calculate the volume of additional control packets.

The average communication overhead additionally generated for detecting and excluding the nodes with abnormal activities as shown in **Fig. 14** was approximately 2-5 % compared to the total communication traffic in this experimental environment. However, we think this value is acceptable considering that the proposed solution provides from 10 to 20% more throughput than the existing scheme. Additionally, the control packet communication

overhead decrements as the misbehaving nodes are excluded from the network. This means that the proposed solution is profitable considering the augmented throughput and the continuously decreasing control packet overhead.

5. Security Analysis

5.1 Analysis of False positives caused by Communication Errors

In this paper, we have assumed that nodes are deployed in a secure communication environment where the nodes can overhear perfectly packet transmissions of neighbor nodes. However, in an ad-hoc network environment, it is possible the occurrence of the exclusion of normal nodes caused by false positives because of overhearing failures caused by different types of communication errors. Therefore, we have make an analysis in respect to this issue.

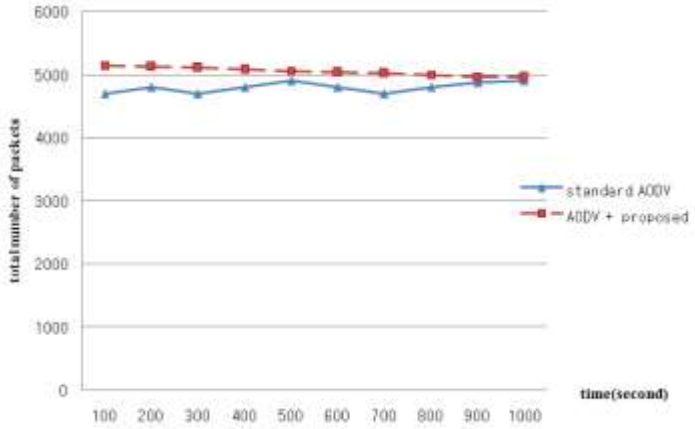

Fig. 14. Communication overhead of the proposed solution

The **Fig. 15** shows the result of the normal nodes excluded erroneously in a network with 10% of misbehaving nodes and variable communication error rate. The maximum rate of communication error considered for the simulation was 10%.

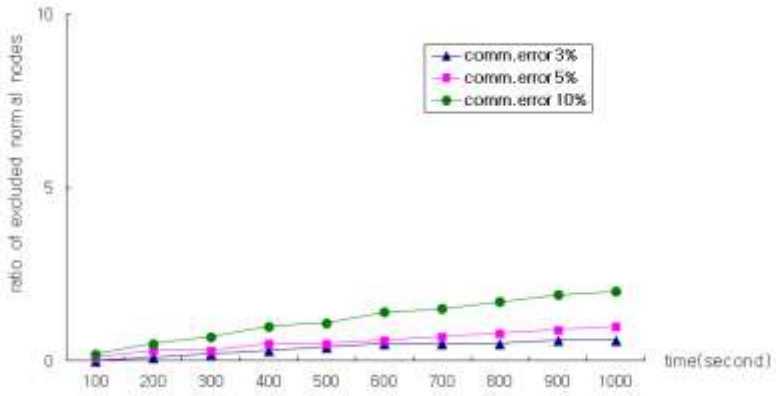

Fig. 15. Ratio of normal nodes excluded by false positives caused by communication error

The result shows that even though the normal nodes receives negative weights because of communication error, the relief algorithm allows them to recover rapidly its weight to the normal levels.

5.2. Analysis of False Positives and False Negatives with Different Thresholds

In this paper, the NWMS node manages the weight of misbehaving nodes using the information collected from the NWARN messages sent by low level nodes. If an abnormal behaviour of a node is detected, its weight is increased, and if such value reaches higher value than a threshold, the misbehaving node is excluded from the network. The results related with false positives and false negatives with different thresholds are shown in **Fig. 16** and **17**, respectevely. The figures illustrate the statistical results after executing 30 simulations with 10% of misbehaving nodes. The results indicates that if the threshold value is lower than 5, misbehaving nodes are detected fast which is an advantage; however, it also involves the problem of rapid increase of false positives. On the other hand, if the threshold is higher than 5, the exclusion of normal nodes caused by false positives are avoided; however, it incorporates the problem that the misbehaving nodes can downgrade the throughput of the network because they are not detected during a long period of time. Through this experimentation, we could observe that a optiomal value of the threshold was 5. However, the posibility of its optimization remains for future works.

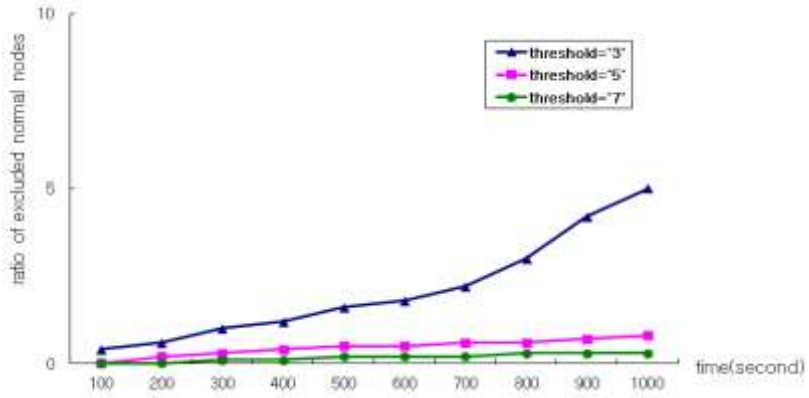

Fig. 16. Ratio of normal nodes excluded because of false positives with different thresholds

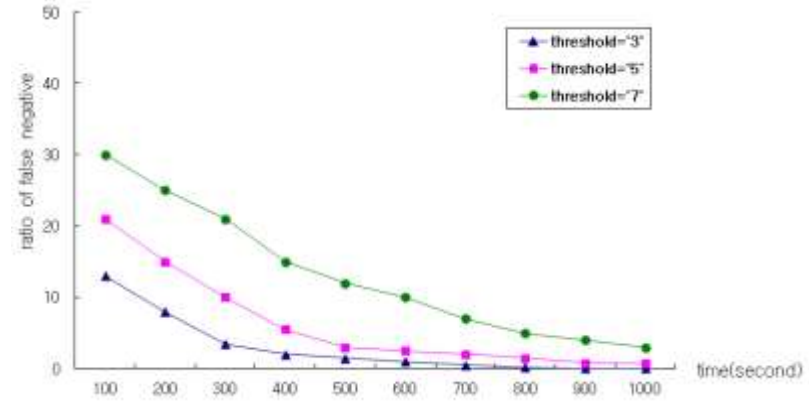

Fig. 17. Ratio of misbehaving nodes not excluded by false negative with different thresholds

6. Conclusion

The ad-hoc network could not directly apply the existing security mechanism because it does not have a fixed infrastructure and it is composed of mobile nodes with insufficient operational capability and small battery capacity. Since the network is constructed based on a premise of cooperative relations with each other, although the participants in the communication are many unknown nodes, there are security vulnerabilities. In addition, the existing presented detection techniques have a problem that did not completely consider the malicious nodes with false accusations. Accordingly, this paper presented the technique to detect and exclude simultaneously the malicious nodes with false accusations as well as the nodes with usual abnormal activities, and verified the network efficiency through an experiment. In general, the ad-hoc network for tactical communication is differentiated from the traditional ad-hoc network in the following aspect; the initial participants in the communication could be composed of reliable nodes, and it is decided that some part could be arranged in a hierarchy due to the property of the nodes used.

Therefore, this paper exploited the upper layer' nodes as the NWMS servers to manage the weight of each node in the area, so that they could quickly detect and exclude the nodes with abnormal activities. In addition, the optimum reliable multiple paths could be established by exploiting the SNL managed by each node in the path establishment stage. The solution was additionally presented as applying the ElGamal scheme to solve the vulnerability due to the collusive nodes, and the algorithm to reduce the weight for maintaining the survivability of the nodes to which the unfair weights were assigned was also presented.

As a result of the simulation according to the method proposed in this paper, it could be confirmed that the throughput of the overall network is improved by effective detection and exclusion of the malicious nodes with false accusations. In the future, additional experiments and study are planned to examine whether or not the technique proposed in this paper can effectively detect a variety of threats for ad-hoc networks.

References

[1] P. Michiardi, and R. Molva, "Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks," in *Proc. of European Wireless 2002 Conference*, 2002.

[2] Y. Zhang, and W. Lee. "Intrusion detection in wireless ad-hoc networks," in *Proc. of 6th ACM Annual International Conference on Mobile Computing and Networking*, pp.275-283, Aug.2000. Article (CrossRef Link)

[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. of 6th ACM Annual International Conference on Mobile Computing and Networking*, pp.255-265, Aug.2000. Article (CrossRef Link)

[4] S. Buchegger, and J-Y. L. Boudec, "Nodes Bearing Grudges: towards routing security, fairness and robustness in mobile ad hoc networks," in *Proc. of 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing*, pp.403-410, Jan.2002. Article (CrossRef Link)

[5] S. Buchegger, and J-Y. L. Boudec, "Performance analysis of the CONFIDANT Protocol," in *Proc. of the 3rd ACM International Symposium on Mobile ad hoc networking & computing*, pp.226-236, 2002. Article (CrossRef Link)

[6] K. Chang, and J-L Chen, "A Survey of Trust Management in WSNs, Internet of Things and Future Internet," *KSII Transactions on Internet and Information System*, vol.6, no.1, pp.5-23, Jan.2012

[7] P. Kyul, H. Nishiyama, N.Ansari, and N. Kato, "certificate revocation to cope with false accusations in mobile ad hoc networks," in *Proc. of 71st IEEE Vehicular Technology Conference*, pp.1-5, May,2010. Article (CrossRef Link)

[8] A. Kathirvel, and R. Srinivasan, "Self_USS:A self umpiring system for security in mobile ad hoc

network," *International Journal of Engineering and Technology*, vol.2, no.2, pp.196-203, Apr.2010.
[9] C. Tseng, T. Song, P. Balasubramanyam, A. Ko, and K. Levitt, "A specification-based Intrusion Detection Model for OLSR", *LNCS*, vol.3858, pp.330-350, 2006. Article (CrossRef Link)
[10] A. Mitrokotsa, R. Mavropodi, and C. Douligeris, "intrusion detection of packet dropping attacks in mobile ad hoc networks," in *Proc. of International Conference on Intelligent Systems and Computing: Theory And Applications*, pp.111-118, Jul.2006.
[11] O. Gonzalez, G. Ansa, M. Howarth, and G. Pavlou, "Detection and accusation of packet forwarding misbehavior in mobile ad-hoc networks," *Journal of Internet Engineering*, pp.181-192, Jun.2008.
[12] J. Sen, and K. Goswami, "An algorithm for detection of selfish nodes in wireless mesh networks," in *Proc. of the International Symposium on Intelligent Information Systems and Applications*, pp.571-576, Oct.2009.
[13] T. Anantvalee, and J. Wu, "A survey on intrusion detection in mobile ad hoc networks," *Book Series Wireless Network Security, Springer*, pp.170-196, 2007.
[14] V. Gokhole, S.K. Ghosh, and A. Gupta, "classification of attacks on wireless mobile ad hoc networks and vehicular ad hoc networks," *Taylor and Francis Group, eBook*, pp.195-225, 2011.
[15] C. K. Toh, E.C. Lee, and N.A. Ramos, "Next-Generation Tactical Ad Hoc Mobile Wireless Networks," *NORHTROP GRUMMAN Technology Review Journal*, pp.103-116, Spring/Summer 2004.
[16] J. Brand, and G. Hartwig, "Management of tactical ad hoc networks with C2 data models," in *Proc. of MILCOM 2001*, pp.915-922, Aug.2001. Article (CrossRef Link)
[17] M. Popa, C. Moica, A.S. Popa, D. Mnerie, "Hierarchical Ad Hoc Networks", in *Proc. of IEEE EUROCON 2007, The International Conference on "Computer as a Tool"*, pp.2509-2516, 2007. Article (CrossRef Link)
[18] S-J. Yoon, S-H. Lee, Y-B. Ko, "Reliable dual-path geocasting for tactical ad hoc networks," in *Proc. of MILCOM 2009*, pp.1-7, Oct.2009. Article (CrossRef Link)
[19] H. Wang, Y. Wang, J. Han, "A security architecture for tactical mobile ad hoc networks," *in Proc. Of IEEE 2nd International Workshop on Knowledge Discovery and Data Mining*, pp.312-315, Jan.2009. Article (CrossRef Link)
[20] F.R. Yu, H. Tang, P.C. Mason, Wang Fei, "A hierarchical identity based key management scheme in tactical mobile ad hoc networks," *IEEE Transactions on Network and Service Management*, vol.7, no.4, pp.258-267, Dec.2010. Article (CrossRef Link)
[21] S-W. Lee, J. Y. Choi, K. W. Lim, Y-B. Ko, and B-H. Roh, "a reliable and hybrid multi-path routing protocol for multi-interface tactical ad hoc networks," in *Proc. of MILCOM 2010*, pp.2237-2242, Nov.2010. Article (CrossRef Link)
[22] C. E. Perkins, and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proc. of 2nd IEEE Workshop on Mobile Computer Systems and Applications*, pp.90-100, Feb., 1999. Article (CrossRef Link)

Yunho Lee received his B.S. in Electronic Engineering from Korea Military Academy in 1999, M.S. in Computer Engineering from Seoul National University, Korea, in 2005. Currently, he is a Ph.D. course in Defense Information Science, Korea National Defense University. His research interests include mobile network security, key management and intrusion detection.

Sang-Guun Yoo received the B.Eng. and M.S. degrees from Escuela Politécnica del Ejército (Ecuador) and Sogang University (Korea) in 2002 and 2010, respectively. He is one of the co-founders of ExtremoSoftware (Microsoft Gold Certified Partner) where worked as IT architect from 2001 to 2005. From 2005 to 2007, he worked as a research member and professor in Department of Computer Science and Multimedia of International University of Ecuador. He also worked as an external IT consultant for the Army Intelligence Agency of Ecuador from 2006 to 2007. He is currently pursuing the Ph.D. degree at the Department of Computer Science and Engineering at Sogang University.

Soojin Lee received his B.S. in Computer Science from Korea Military Academy in 1992, M.S. in Computer Science from Yonsei University, Korea, in 1996, and Ph.D. in Computer Science from Korea Advanced Institute of Science and Technology (KAIST), Korea in 2006. Since 2006, he has been an associate professor at the Dept. of Defense Information Science, Korea National Defense University. His research interest includes computer and communication security, intrusion detection, and mobile network security.