

Historical Evidence Based Trust Management Strategy against Black Hole Attacks in MANET

Bo YANG^a, Ryo YAMAMOTO^a, Yoshiaki TANAKA^{a,b}

^a Global Information and Telecommunication Institute, Waseda University, Japan

^b Research Institute for Science and Engineering, Waseda University, Japan
yangbo_youhaku@ruri.waseda.jp

Abstract— Distributed, self-organized and infrastructure-independent nature of MANET makes it vulnerable to various kinds of attacks. Among them, a threat caused by black hole attack is more prominent. A trust management scheme is a common way to detect and isolate the compromised nodes while a cryptography mechanism shows a failure facing to inner attacks. The previous work proposed two simple models along with trust computation methods to filter out black hole nodes using the benevolent ones and achieved better performance against pure black hole attacks. In this study, a method to prevent gray hole attack, one kind of black hole attack, which is more cunning and clandestine attack is proposed. The neighbour observing model based on watchdog concept is focused on the direct trust value (DTV) to detect single black hole attack. Historical evidence is also taken into consideration against gray hole attacks. Moreover, the neighbour recommendation model that accompanied with indirect trust value (ITV) is used to detect the cooperative black hole attacks. On the other hand, the proposed method tries to balance the trust values from different neighbour nodes to mitigate the damage by their deceiving. The simulation results demonstrate the advantages of proposed method by punishing malicious actions to prevent the camouflage and deception in the attack.

Keywords— Historical evidence, Trust management strategy, Direct trust value, Indirect trust value, Black hole attack, Grey hole attack, MANET

I. INTRODUCTION

The mobile ad hoc network (MANET) is being implemented in various scenarios such as military surveillance, disaster relief, chemical leakage monitoring, forest fire monitoring. However, MANET makes it particularly vulnerable for various attacks compared with conventional networks due to its flexibility and infrastructure-independent nature. Security problems in MANET are mainly aroused by its unique characteristic such as dynamic network topology, limited bandwidth and limited battery power. As concern this, a cryptography mechanisms, intrusion detection system (IDS) and efficient routing protocols are proposed to ensure the security of ad hoc networks. However, these conventional methods, especially cryptography method, fail when they try to eliminate compromised nodes from the legitimated ones. Although lots of efficient routing protocols are proposed to ensure the security of the ad hoc network, routing attacks are still harmful. Moreover, the malicious nodes can launch routing attacks to deprive the routing path and relative operation that causes catastrophic damage to normal communication of a large area in the network. The study is

focused on the black hole attack that malicious nodes pretend as if they have the shortest path to the destination. However, most of them either spends a large overhead or cannot prevent the cooperative black hole attack effectively.

In order to detect a single black hole attack as well as a cooperative black hole attack, a neighbour nodes observation model (NNOM) and a neighbour recommendation trust model (NRTM) based on the former one is given in our previous study [1]. The method introduces a trust mechanism to filter inner attackers in ad hoc network. The NNOM is based on the watchdog mechanism [2] and each node keeps on watching its own neighbour nodes while judging its communication behaviour. These statistical data are used to compute a direct trust value (DTV) which is compared with a predefined threshold to decide whether a neighbour node is a malicious node or not. Even if a neighbour node acts as a normal node, the node is not trusted immediately since the next hop of the node considers the case that a cooperative black hole attack is hidden behind. That is, the NRTM is established among the nodes and the other neighbour nodes are asked to declare their opinion about the reputation of the two hop neighbour node. Furthermore, an indirect trust value (ITV) is computed and simply compared with a predefined threshold to decide whether there is a cooperative black hole attack.

Malicious nodes may act abnormally after a long period normal actions and their reputation still remains high. It is known as another type of black hole attack: gray hole attack, which is taken in certain time period or to certain data packets. This kind of attack is more harmful and even more difficult to detect because of their malicious behaviour. In this paper, historical evidence based NNOM and DTV based on the Dempster-Shafer (D-S) evidence theory [3] are proposed to settle this problem. The proposed method makes it difficult for each node to get a high reputation after a long run, but easy to lose it. Moreover, the recommended reputation from some neighbour nodes with ulterior motives might confuse the final judgement of the mechanism. The proposed method considers the data distance between two reputation evidences [4] and that makes the cheating impact on ITV minimize.

The rest of this paper is organized as follows. In section II, the single black hole attack and the cooperative black hole attack is introduced. Then related work is described. In section III, details of the proposed model and algorithms along with the processes step of the strategy is described. The numerical result and the simulation study are analyzed in section IV. Finally, section V concludes this paper.

II. BLACK HOLE ATTACK AND RELATED WORKS

A. Black Hole Attack and Gray Hole Attack

Varieties of routing protocol are implemented in the MANET that can be classified into three categories: proactive, reactive, and hybrid. Some famous and representative ones are destination sequence distance vector (DSDV) as proactive protocol, and dynamic source routing (DSR) along with ad hoc on-demand distance vector (AODV) as reactive protocol [5]. Reactive routing protocols such as AODV initiate a route discovery process at the beginning of a communication when there is no valid and fresh route from the source node to the destination node. In this process, destination sequence numbers and unique broadcast IDs are used to ensure that the routes are loop-free and freshness of the routes. The source node broadcasts route request (RREQ) packets to all its neighbour nodes and the packets are relayed to next hop node until legitimated destination node receives them. After receiving RREQ, the destination node or an intermediate node with fresh route to the destination responds it by unicasting a route reply (RREP) packet. When the source node receives the RREP packet, the route is established and the communication between the source node and the destination node is done though the route.

In this route discovery phase, two types of black hole attack can be found: single attack and cooperative attack. The attacks can be aroused in two phases: the RREQ phase and the RREP phase. In this paper, the proposed method focuses on the black hole attack in the RREQ phase and the behaviour of malicious nodes in that period.

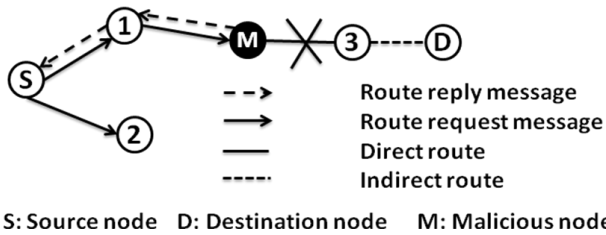


Figure 1. Single black hole attack

As is shown in Figure 1, a single black hole attack is done merely by one malicious node. When a malicious node M receives RREQ message from the source node S, it sends back fallacious RREP message immediately without relaying it to the real destination node D through node 3. Since the malicious nodes gerrymander the sequence number and the ID number, node S is convinced that node D is the next hop of node M. In this way, the malicious node is able to collect all the packets from the source node and do further actions such as dropping them or analysing the data. In order to tackle this problem, some conventional methods are proposed to settle this kind of problem by monitoring the neighbour nodes' activity. However, it does not work properly when two or more malicious nodes cooperate together.

Figure 2 shows an example of cooperative attack with malicious node M_1 and M_2 . When the source node S tries to find a route to the destination node D, it broadcasts RREQ to the destination node. Since node 2 might watches the

behaviour of node M_1 closely, M_1 tries to pretend to be a normal node and just relay the RREQ to node M_2 . After node M_2 receives RREQ from node M_1 , it begins malicious action that is the same as the single attack. In this way, node M_1 and M_2 can hide in the network without being noticed by other normal nodes. For the cases of more than two malicious nodes in the network, the harmful influence becomes greater since the prevention becomes much difficult.

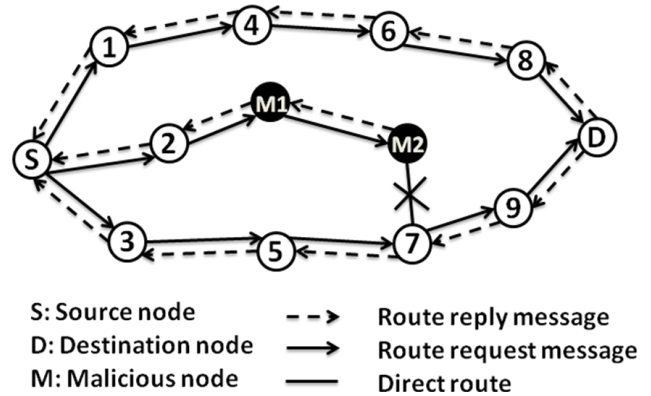


Figure 2. Cooperative black hole attack

More harmful type of attacks in black hole attack is the gray hole attack [6]. The significant difference between the gray hole attack and black hole attack is that the former one only does the action in certain time period or to certain data. A gray hole attack node firstly exploits the route by advertising it has the shortest path to the destination node, then the node can establish the route through it. By doing this, it may be able to drop packets from a certain target node in for some time duration. However, it turns to normal behaviour for other nodes to hide its malicious presence for most of the time. In some other case, the malicious node may do attack to some certain data from the target node. Therefore, the gray hole attack becomes more difficult to detect than the ordinary black hole attack.

B. Related Works

In our previous work, each node implements a global agent acting as a watchdog that detects the packets relaying of neighbour nodes [7], [8]. The model is called NNOM as is seen in Figure 3. In this figure, node 1 keeps on watching node 2, 3, 4 and M. When node M drops packets, the observation nodes begin to observe its abnormal behaviour and calculate DTV based on the statistical data of node M's behaviour by using following Eq. (1):

$$D_i(j) = \frac{S}{S + F}, \quad (1)$$

where:

$D_i(j)$ represents the DTV of node j judged by node i ;
 S is the number of successful packets relayed by node j ;
 F is the number of failed packets relayed by node j .

Once DTV becomes lower than a predefined threshold D_{th} , the node is treated as a malicious node. It is apparent that when the black hole node takes action all the way, S becomes

smaller compared with F . That is, the DTV decrease sharply along with the passage of time.

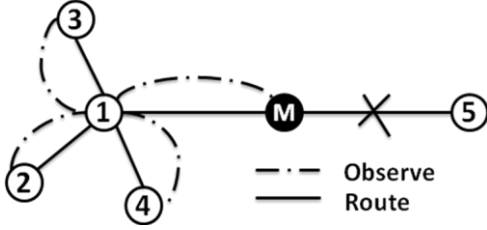


Figure 3. Neighbour nodes observation model (NNOM)

For the case of gray hole attack, however, long terms of normal behaviour may help the malicious node to get a higher DTV. Since the attack nodes in a gray hole attack is intermittently, the malicious node act as normal as possible to earn higher DTV all the way. Irregular malicious behaviour does not decrease the DTV obviously, thus the node is treated as normal node.

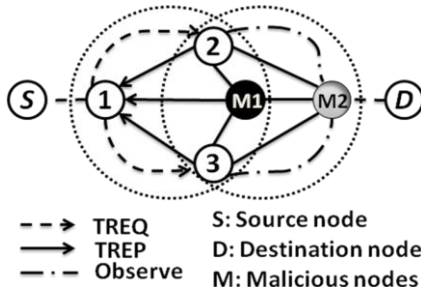


Figure 4. Neighbour recommendation trust model (NRTM)

In order to detect two cooperative malicious nodes, NRTM [9] is proposed as is shown in Figure 4. When M_1 acts normal, node 1 does not trust it directly. However, it tries to get other neighbour nodes' opinion about node M_2 . Trust request (TREQ) message and trust reply (TREP) message are introduced to accomplish this requirement [10]. Firstly, the node 1 broadcasts TREQ messages to its neighbour nodes 2, 3. The nodes which receive TREQ reply TREP with $D_j(k)$ of M_2 immediately. After a recommendation time to live (RTTL), the ITV is calculated using the following Eq. (2):

$$I_i(k) = \frac{\sum_{j \in N_i, j \neq m} D_i(j) D_j(k)}{|N_i| - 1} \leq 1, \quad (2)$$

where:

- $I_i(k)$ represents the ITV of node k judged by node i ;
- $D_i(j)$ is the DTV of node j judged by node i ;
- $D_j(k)$ is the DTV of node k judged by node j ;
- N_i is the neighbour nodes' set of node i ;
- m is the suspicious node between node i and node k .

ITV is stored in an indirect trust table (ITT) and compared with a predefined threshold I_{th} . If ITV is lower than I_{th} , the node M_1 along with node M_2 are recognized as a malicious node. Then, the ID of node M_1 and M_2 are added to node 1's malicious table and restart the route discovery phase. However, some intermediate neighbour nodes may lie to the observation node and that affect the judgment of observation node on two hop neighbour node. For example, if node 2 may

give a high reputation of node M_2 , it increases ITV and becomes insensitive to the attack actions of the malicious nodes. If the number of recommendation nodes becomes large, the node M_2 is never to be considered as malicious node.

III. PROPOSED MODELS AND ALGORITHMS

A. Proposed NNOM and DTV

Our previous work only considers about the communication factors such as routing packets as well as data packets. Moreover, it is supposed that each node only marks its neighbour nodes with cooperative and uncooperative by calculating DTV [11]. However, the watchdog mechanism usually considers about safety data fusion, which is used to make sure data's integrity that sent data and received data are exactly the same. In this case, a nodes' behaviour can be classified into three categories: normal, suspicious, and malicious. The proposed method supposes that each node watches its neighbour node and marks its behaviours as α , β and γ : the number of benevolent, malicious and suspicious respectively in a certain time period respectively. The target of the proposed method is to make it more difficult for a node to get a higher reputation in a long run while easy to lose it. The proposed method also takes historical evidence into consideration. It is inspired by the Dempster-Shafer (D-S) evidence theory, which is an effective method of combining accumulative evidences or for changing priors in the presence of new evidences [12].

The proposed DTV algorithm can be described in following Table 1. This algorithm decides whether neighbour node is a malicious node or not.

TABLE 1. DTV ALGORITHM

DTV Algorithm
Step 1: Node i watches node j from T_n to T_{n+1}
Step 2: $(\Delta\alpha, \Delta\beta, \Delta\gamma)$ is calculated
Step 3: Compare $\Delta\alpha$ and $\Delta\beta$ to decide the value of θ using Eq. (6)
Step 4: Calculate the trust evidence $(\alpha_{n+1}, \beta_{n+1}, \gamma_{n+1})$ at T_{n+1} using Eq. (3)-(5)
Step 5: Calculate the DTV of node j using Eq. (7)-(10)
Step 6: if $B_{i,j} - M_{i,j} < \eta_1$ and $S_{i,j} < \varepsilon_1$ node j is trusted else if $B_{i,j} - M_{i,j} > \eta_2$ and $S_{i,j} < \varepsilon_1$ node j is malicious node and put into MT. else node j is listed on ST
End.

From a time period $[T_n, T_{n+1}]$, each node i counts a recent trust evidence of its neighbour node j . The trust evidence is refreshed from time T_n to T_{n+1} using the following Eq. (3) to Eq. (5). The refresh weight θ is decided by newly counted trust evidence using following Eq. (6). In order to punish the malicious actions, a high value is given to θ_n . In order to prevent the camouflage and deception, lower θ_i is used. The value of θ_n and θ_i is in the range of $0 < \theta_i < 0.5 < \theta_n < 1$.

$$\alpha_{n+1} = (1 - \theta)\alpha_n + \theta\Delta\alpha, \quad (3)$$

$$\beta_{n+1} = (1 - \theta)\beta_n + \theta\Delta\beta, \quad (4)$$

$$\gamma_{n+1} = (1 - \theta)\gamma_n + \theta\Delta\gamma, \quad (5)$$

$$\theta = \begin{cases} \theta_l, & \text{if } \Delta\alpha \geq \Delta\beta \\ \theta_h, & \text{if } \Delta\alpha < \Delta\beta \end{cases} \quad (6)$$

where:

- $\Delta\alpha$ is the number of the normal behaviours in $[T_n, T_{n+1}]$;
- $\Delta\beta$ is the number of the malicious behaviours in $[T_n, T_{n+1}]$;
- $\Delta\gamma$ is the number of the suspicious behaviours in $[T_n, T_{n+1}]$;
- α_n is the trust evidence of normal behaviour at T_n ;
- β_n is the trust evidence of malicious behaviour at T_n ;
- γ_n is the trust evidence of suspicious behaviour at T_n ;
- θ is the refresh weight.

Based on the trust evidence that cares about the historical data, DTV is calculated using following Eq. (7) to Eq. (10):

$$B_{i,j} = \frac{\alpha_n}{\alpha_n + \beta_n + \gamma_n}, \quad (7)$$

$$M_{i,j} = \frac{\beta_n}{\alpha_n + \beta_n + \gamma_n}, \quad (8)$$

$$S_{i,j} = \frac{\gamma_n}{\alpha_n + \beta_n + \gamma_n}, \quad (9)$$

$$D_{i,j} = (B_{i,j}, M_{i,j}, S_{i,j}), \quad (10)$$

where:

$B_{i,j}$ represents the benevolent actions DTV of node j at T_n ;
 $M_{i,j}$ represents the malicious actions DTV of node j at T_n ;
 $S_{i,j}$ represents the suspicious actions DTV of node j at T_n .
 DTV of node j calculated by node i is represented by $D_{i,j}$, which consists of three parts: $B_{i,j}$, $M_{i,j}$, $S_{i,j}$. Each node maintains two tables: Malicious Table (MT) and Suspicious Table (ST). If a neighbour node is considered to be malicious node, the observation node records its node ID in MT. If there is not enough evidence to make sure whether it is normal or malicious at the very moment, its ID is recorded in the ST of the observation node. Relative thresholds are described in the Step 6 of the DTV algorithm. DTV is stored in a Direct Trust-value Table (DTT) for further use in ITV.

B. Proposed NRTM and ITV

Using the proposed DTV, the route through one neighbour node is not be set up directly when it is trusted by the observe nodes. As is shown in figure 5, node i tries to get other neighbour nodes' opinion about the next hop of node j , namely, node k . For this reputation, node i broadcasts TREQ messages to get the DTV of node k . In a predefined recommendation time to live (RTTL), the neighbour nodes such as nodes P_1 , P_2 and P_3 send back TREP messages including DTVs of node k . Then, DTV of neighbour nodes and DTV of node k are used together to calculate ITV. However, some of the neighbour nodes may deceive node i by giving a high reputation of node k . Therefore, the proposed method tries to give each neighbour node an evaluation difference to balance the neighbour node's cheating enhancements on the value of ITV. The proposed ITV calculation algorithm is described in following Table 2 whether there are cooperative black hole attack or not.

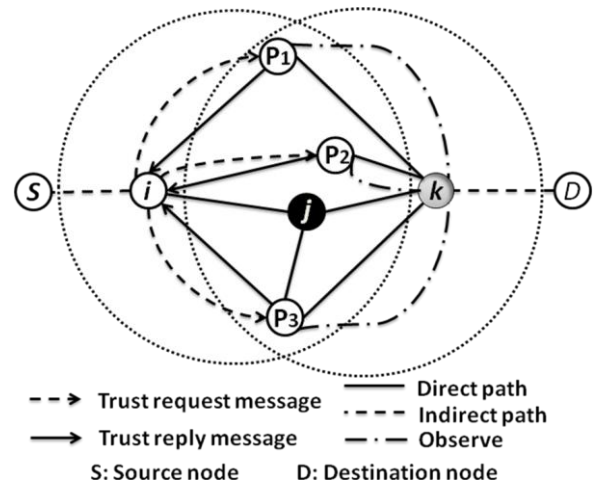


Figure 5. Neighbour recommendation trust model (NRTM)

TABLE 2. ITV ALGORITHM

ITV Algorithm

- Step 1: Do DTV algorithm on node j , if it acts normal go on to step 2
- Step 2: Node i asks nodes p 's DTV on node k
- Step 3: Calculate the evaluation difference using Eq. (11)-(13)
- Step 4: Calculate the ITV of node k using Eq. (14)-(17)
- Step 5: if $b_{i,k} - m_{i,k} < \delta_1$ and $s_{i,j} < \varepsilon_2$
 node k is trusted
 else if $b_{i,k} - m_{i,k} > \delta_2$ and $s_{i,j} < \varepsilon_2$
 node k is malicious node and put into MT.
 else node k is listed on ST
- End.

The evaluation difference based on the data distance [13], which means each two data's difference, is calculated by following Eq. (11) to Eq. (13). The evaluation difference of each part in DTV is represented as d_B , d_M , d_S and the range is $[0,1]$ and smaller difference makes them closer to 0.

$$d_B = \frac{\sum_{q \in N_i, q \neq j, q \neq p} |B_{i,q} B_{q,k} - B_{i,p} B_{p,k}|}{|N_i| - 2}, \quad (11)$$

$$d_M = \frac{\sum_{q \in N_i, q \neq j, q \neq p} |M_{i,q} M_{q,k} - M_{i,p} M_{p,k}|}{|N_i| - 2}, \quad (12)$$

$$d_S = \frac{\sum_{q \in N_i, q \neq j, q \neq p} |S_{i,q} S_{q,k} - S_{i,p} S_{p,k}|}{|N_i| - 2}, \quad (13)$$

where:

- d_B represents the evaluation difference of B in DTV;
- d_M represents the evaluation difference of M in DTV;
- d_S represents the evaluation difference of S in DTV;
- N_i is the neighbour nodes set of node i .

Based on the evaluation difference, each neighbour node can be given a different trust weight to calculate the ITV. Take d_B for example, if a given $B_{i,p} B_{p,k}$ is more different from other $B_{i,q} B_{q,k}$, the d_B of this recommendation reputation is larger than

other ones. Then, this recommendation reputation may be given by a deceiving nodes and a low trust weight is used to decrease its impact on total ITV as is shown in the following Eq. (14) to Eq. (17):

$$b_{i,k} = \frac{\sum_{p \in N_i, p \neq j} B_{i,p} B_{p,k} (1-d_B)}{|N_i|-1}, \quad (14)$$

$$m_{i,k} = \frac{\sum_{p \in N_i, p \neq j} M_{i,p} M_{p,k} (1-d_M)}{|N_i|-1}, \quad (15)$$

$$s_{i,k} = \frac{\sum_{p \in N_i, p \neq j} S_{i,p} S_{p,k} (1-d_S)}{|N_i|-1}, \quad (16)$$

$$I_{i,k} = (b_{i,k}, m_{i,k}, s_{i,k}), \quad (17)$$

ITV of node k calculated by node i is represented by $I_{i,k}$, which consists of three parts: $b_{i,k}$, $m_{i,k}$, $s_{i,k}$. The value of ITV is stored in an Indirect Trust-value Table (ITT). According to the Step 5 in the ITV algorithm, if node k is trusted, the source node establishes the route though node j and node k . If not, node k is stored in the MT as a malicious node.

IV. PERFORMANCE EVALUATION

A. Evaluation 1: Numerical Analysis

Performance evaluation is firstly conducted to study the proposed DTV and ITV from the aspect of numerical analysis. Matlab is used as an analyzer. For DTV algorithm, α_0 , β_0 and γ_0 are set to 1 at initial phase. In each time period $[T_n, T_{n+1}]$, we give a set of evaluation evidences for three kinds of nodes: normal nodes, black hole nodes, gray hole nodes. For ITV algorithm, the gray hole node is supposed to act as normal nodes for the first 10 rounds and then begin to take malicious actions for two rounds and tries to act normal again. It is supposed that each recommendation node is given $B_{i,p}=0.8$. If a recommendation node is trying to deceive, set $B_{p,k}$ to 0.9. Otherwise, set $B_{p,k}$ to 0.1. The number of deceiving node is 10. Other parameters are set based on the simulation.

1) DTV Performance Evaluation:

Fig. 6 shows the performance of DTV with the gray hole node. As is described in the simulation environment, the gray hole node firstly acts as a normal node in the first 10 rounds. The malicious node takes action from 10th round to 12th round. After that, the gray hole node acts as normal as possible. As is described previously, the DTV of a neighbour node j calculated by node i consists of three parts: $B_{i,j}$, $M_{i,j}$ and $S_{i,j}$. It is apparent that $B_{i,j}$ decreases sharply while $M_{i,j}$ increases immediately. Meanwhile, $B_{i,j}-M_{i,j}$ also drops from 0.6 to minus 0.8 at the same time. However, $B_{i,j}-M_{i,j}$ along with $B_{i,j}$ increase at a very low speed compared with their decrease of the value. It is easy to find that the proposed method makes it difficult for the gray hole node to get a high reputation: DTV. The mechanism is so sensitive that DTV changes dramatically whenever the node drops packets. However, it is difficult to restore its former reputation in a short time period. Based on the numerical analysis of DTV, we set some key parameters in

the decision part of the DTV algorithm: $\eta_1=0.4$, $\eta_2=-0.6$ and $\varepsilon_1=0.2$.

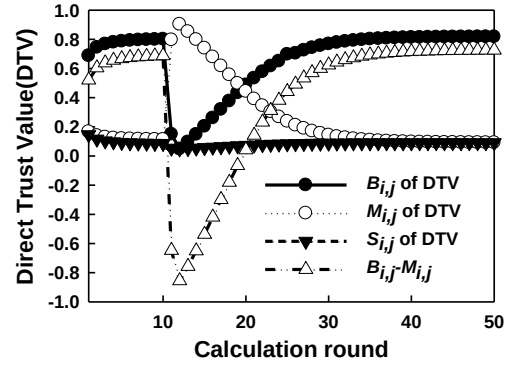


Figure 6. Transition of DTV with gray hole node

2) ITV Performance Evaluation:

Fig. 7 shows the performances of ITV influenced by the deceiving nodes. For the proposed ITV, it is set that there are totally 10 nodes acting as the recommendation nodes, among which 3 nodes are cheating. As is described previously, the ITV of a two-hop neighbour node k calculated by node i consists of three parts: $b_{i,k}$, $m_{i,k}$ and $s_{i,k}$. $b_{i,k}$ is increasing in a low speed but still no more than 0.25. $m_{i,k}$ decreases but always maintains higher than -0.15. $s_{i,k}$ changes slightly from 0.04 to 0.06, approximately. After the proposed ITV is implemented, although those deceiving nodes keep on cheating, the values of $b_{i,k}$, $m_{i,k}$, and $s_{i,k}$ change slowing. The enhancement of the false DTV is minimized. Based on the numerical analysis of ITV, we set some key parameters: $\delta_1=0.6$, $\delta_2=0.4$ and $\varepsilon_2=0.06$.

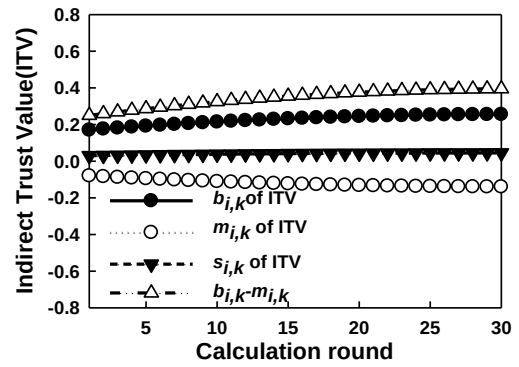


Figure 7. Transition of ITV with deceiving node

B. Evaluation 2: Network Simulation

As a second evaluation, the proposed mechanism is implemented in AODV using simulator GloMoSim2.03 to study the detection rate. The parameters are set as Table 4.

1) DTV Performance Evaluation:

Fig.8 shows the detection rate of the gray hole nodes. PDTV stands for past DTV method while NDTV means the proposed DTV method. The detection rate of the malicious node decreases with the increase of the nodes' moving speed.

TABLE 3. SIMULATION PARAMETERS

Simulator	GloMoSim2.03
Routing protocol	AODV
Mac protocol	IEEE 802.11
Simulation area	1000m×1000 m
Node placement	Random
Number of nodes	50
Transmission range	180m
Maximum speed	10m/s
Traffic type	CBR (UDP)
Packet rate	2 packets/s
Data payload	512bytes/packets
Pause Time	30s
Simulation Time	1000s
Mobility Model	Random waypoint

Faster moving speed makes them difficult to gather the information of their neighbour nodes and that causes the performance degradation. Moreover, the previous method has almost no resilience facing the gray hole attack while the evidence-based proposed DTV shows better performance.

2) ITV Performance Evaluation:

Fig.9 shows the detection rate of cooperative black hole nodes with deceiving nodes. The detection rate of the malicious node decreases with the increase of the node's moving speed. PITV stands for previous ITV method in our former paper while NITV means the proposed ITV method. NITV shows better detection rate against PITV.

V. CONCLUSIONS

In this paper, the problem of black hole attack and gray hole attack are discussed and two algorithms, NNOM-based DTV and NRTM-based ITV, are proposed. The proposed DTV can be used to detect the gray hole attacks in the networks. The proposed ITV aims at the recommendation of cheating neighbour nodes. However, if there is no such recommendation node or the cheating nodes are too many, the proposed ITV may not take effects. For the future study, it may find another better method instead of the evaluation difference method. Furthermore, we would like to apply this trust management strategy into wireless sensor network (WSN) where the network structure is similar to MANET. However, some other problems such as energy should be taken into consideration.

REFERENCES

- [1] B. Yang, R. Yamamoto, and Y. Tanaka, "A Trust-aware management strategy against black hole attacks in MANET," *IEICE Commun. Society Conf.*, no. BS-6-39, pp S-106-S-107, Sept. 2011.
- [2] S. Ganeriwal, L. K. Balzano, M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Trans. on Sensor Netw.*, vol. 4, pp. 1-37, June 2008.
- [3] A. P. Dempster, "Upper and lower probabilities induced by a multivalued mapping," *The Annals of Mathematical Statistics*, vol. 38, no.2, pp.325-339, April 1967.

- [4] A. L. Jousselme, D. Grenier, E. Bosse, "A new distance between two bodies of evidence," *Information Fusion Journal by Elsevier*, vol. 2, pp.91-101, June 2001.
- [5] D. Djenouri, L. Khelladi, A. N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," *IEEE Communications Surveys and Tutorials*, vol. 7, pp. 2-28, fourth quarter 2005.
- [6] A. D. Wood, J. A. Stankovic, "Denial of service in sensor networks," *Computer Society by IEEE*, vol. 35, pp. 54-62, Oct. 2002.
- [7] S. D. Roy, S. A. Singh, S. Choudhury, "Countering sinkhole and black hole attacks on sensor networks using dynamic trust management," *Computers and Communications by Elsevier*, pp. 537-542, July 2008.
- [8] T. Zahariadis, P. Trakadas, S. Maniatis, "Efficient detection of routing attacks in Wireless Sensor Networks," *Systems, Signals and Image Processing IWSSIP*, pp. 1-4, June 2009.
- [9] H. Chen, "Task-based trust management for wireless sensor network," *Int. J. of Security and Its Applications SERSC*, vol. 3, No. 2, April 2009.
- [10] P. B. Velloso, R. P. Laufer, D. de O Cunha, O. C. M. B. Duarte, G. Pujolle, "Trust management in mobile ad hoc networks using a scalable maturity-based model," *IEEE Trans. on Netw. and Service Management*, vol. 7, pp. 172-185, Sept. 2010.
- [11] B. Y. Yan, F. Y. Liu, M. J. Deng, J. L. Zhou, W. Lu, "Trust model based on risk evaluation in wireless sensor networks," *J. of Central South University*, vol. 42, no. 6, pp. 1657-1662, June 2011.
- [12] J. Cheng, R. J. Feng, X. F. Xu, J. W. Wan, "Trust evaluation model based on D-S evidence theory in wireless sensor networks," *Chinese J. Of Sensors And Actuators*, vol. 22, no. 12, pp. 1802-1807, Dec. 2009.
- [13] Z. Q. Liang, W. S. Shi, "PET: A personalized trust model with reputation and risk evaluation for P2P resource sharing," *Proc. 38th Annual Hawaii Int. Conf. Syst. Sciences, HICSS '05*, pp. 201b-201b, Jan. 2005.

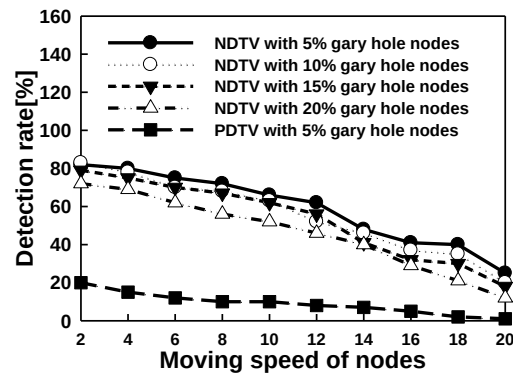


Figure 8. Detection rate with DTV algorithm

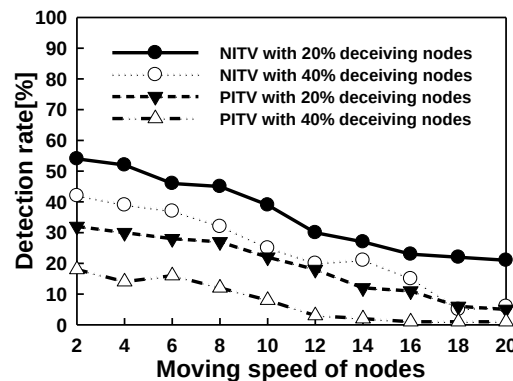


Figure 9. Detection rate with ITV algorithm