Dempster-Shafer Evidence Theory Based Trust Management Strategy against Cooperative Black Hole Attacks and Gray Hole Attacks in MANETs

Bo YANG*, Ryo YAMAMOTO*, Yoshiaki TANAKA*,**

*Global Information and Telecommunication Institute, Waseda University, Japan

**Research Institute for Science and Engineering, Waseda University, Japan

yangbo_youhaku@ruri.waseda.jp, ryo_yamamoto@moegi.waseda.jp, ytanaka@waseda.jp

Abstract—**The MANETs have been experiencing exponential growth in the past decade. However, their vulnerability to various attacks makes the security problem extremely prominent. The main reasons are its distributed, self-organized and infrastructure independent natures. As concerning these problems, trust management scheme is a common way to detect and isolate the compromised nodes when a cryptography mechanism shows a failure facing inner attacks. Among huge numbers of attacks, black hole attack may collapse the network by depriving the route of the normal communication. The conventional proposed method achieved good performance facing black hole attack, while failing to detect gray hole attacks. In this paper, a Dempster-Shafer (D-S) evidence based trust management strategy is proposed to conquer not only cooperative black hole attack but also gray hole attack. In the proposed method, a neighbour observing model based on watchdog mechanism is used to detect single black hole attack by focusing on the direct trust value (DTV). Historical evidence is also taken into consideration to go against gray hole attacks. Then, a neighbour recommendation model companied with indirect trust value (ITV) is used to figure out the cooperative black hole attack. D-S evidence theory is implemented to combine ITVs from different neighbours. Some of the neighbour nodes may declare a false ITV, which effect can also be diminished through the proposed method. The simulation is firstly conducted in the Matlab to evaluate the performance of the algorithm. Then the security routing protocol is implemented in the GloMoSim to evaluate the effectiveness of the strategy. Both of them show good results and demonstrate the advantages of proposed method by punishing malicious actions to prevent the camouflage and deception in the attacks.**

Manuscript received July 25, 2012.

B. YANG is with the Global Information and Telecommunication Institute, Waseda University, Tokyo, 169-0051 Japan. phone: 090-0495-246104; fax: 090-0495-246104; e-mail: yangbo_youhaku@ruri.waseda.jp.

R. YAMAMOTO is with the Global Information and Telecommunication Institute, Waseda University, Tokyo, 169-0051 Japan. e-mail: ryo_yamamoto @moegi.waseda.jp.

Y. TANAKA is with the Global Information and Telecommunication Institute, Waseda University, Tokyo, 169-0051 Japan. He is also with the Research Institute for Science and Engineering, Waseda University, Tokyo, 162-0044 Japan. e-mail: ytanaka@waseda.jp.

Index Terms—**Dempster-Shafer evidence, Trust management, Direct trust value, Indirect trust value, Black hole attack, Gray hole attack, MANETs**

I. INTRODUCTION

The mobile ad hoc networks (MANETs) are flexible networks that inherit common characteristics found in wireless networks in general. However, it adds characteristics specific to ad hoc networks, such as distributed, self-organized infrastructure and mobility. MANETs have been primarily been implemented for tactical network related applications to improve battlefield communications and survivability. Later the technology of MANETs is introduced to some other scenarios such as disaster relief, chemical leakage monitoring, forest fire monitoring, etc. However, owing to its flexibility and infrastructure-independent nature, it is particularly vulnerable to various attacks compared with conventional networks. And security problems in MANETs are mainly aroused by its unique characteristic such as dynamic network topology, limited bandwidth and limited battery power. Concerning about these, cryptography mechanisms, intrusion detection system (IDS) and efficient routing protocols are used to ensure the security of MANETs. However, these conventional methods, especially cryptography method, fail to filter out compromised nodes or the legitimated ones with malicious actions. Although lots of efficient routing protocols are proposed to ensure the security, routing attacks aroused by legitimated nodes that will make the protocols effectiveness. Possible attacks include passive eavesdropping, denial of service (DoS) attacks, wormhole attacks, sybil attacks etc. As one type of DoS attacks, black hole attack can cause catastrophic damage to normal communication of a large area in the network. The black hole nodes can launch routing attacks to deprive the routing path and relative operation such as dropping packets. Most of the existing detection strategy either spends a large overhead or cannot prevent the cooperative black hole attack effectively. This paper focuses

on the black hole attack and gray hole attack that malicious nodes pretend as if they have the shortest path to the destination and then deprive the routing.

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 detect 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) that would be 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 would not be 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 minimized.

The rest of this paper is organized as follows. In section II, the single black hole attack and the cooperative black hole attack are introduced firstly. Then related works are described. In section III the D-S evidence theory is introduced. Section IV describes the details of the proposed model and algorithms along with the processes step of the strategy. The numerical result of algorithms and the network simulation study of security protocol are evaluated in section V and section VI, accordingly. Finally, section VII 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. Then communication between the source node and the destination node would be available 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 the same period.

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

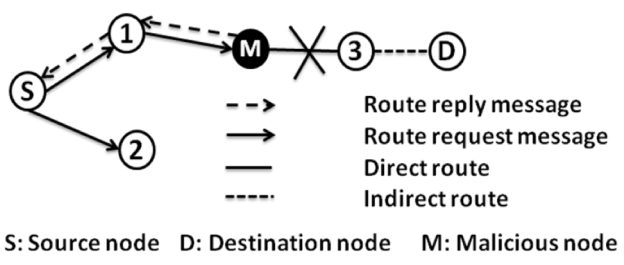


Fig. 1. Single black hole attack

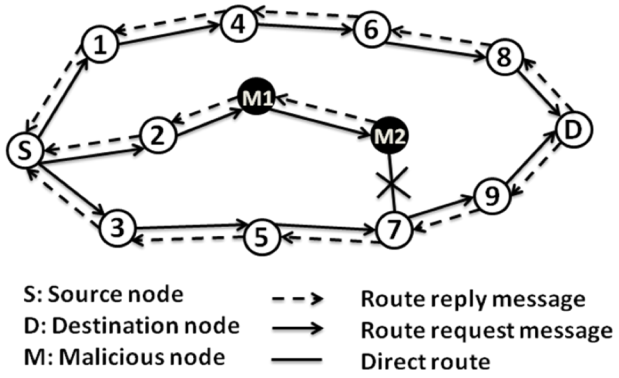


Fig. 2. Cooperative black hole attack

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 illustrates an example of cooperative attack with malicious node M1 and M2. 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 M1 closely, M1 tries to pretend to be a normal node and just relay the RREQ to node M2. After node M2 receives RREQ from node M1, it begins malicious action that is the same as the single attack. In this way, node M1 and M2 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.

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 certain 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 arouse 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. The node 1 calculates DTV on node M based on the statistical data of node M's behaviour by using following Eq. (1):

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

where:

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

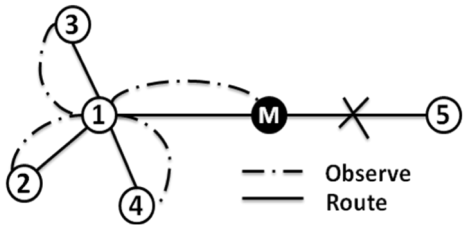


Fig. 3. Neighbour nodes observation model (NNOM)

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.

In order to detect two cooperative malicious nodes, NRTM [9] is proposed as is shown in Figure 4. When M1 acts normal, node 1 does not trust it directly. However, it tries to get other neighbour nodes' opinion about node M2. 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 M2 immediately. After a recommendation time to live (RTTL), the ITV is calculated using the following Eq. (2):

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

where:

$I_i(k)$: the ITV of node k judged by node i;
$D_i(j)$: the DTV of node j judged by node i;
$D_j(k)$: the DTV of node k judged by node j;
N_i: the neighbour nodes' set of node i;
m: 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 M1 along with node M2 are recognized as a malicious node. Then, the ID of node M1 and M2 are added to node 1's malicious table and restart the route discovery phase.

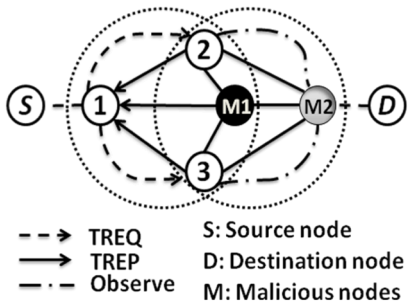


Fig. 4. Neighbour recommendation trust model (NRTM).

However, some intermediate neighbour nodes may lie to the observation node and affect the judgment of observation node on two-hop neighbour node. For example, node 2 may give a high reputation of node M2 compared with other recommender, which makes ITV insensitive to the attack actions of the malicious nodes. Then how to balance the ITVs from different sources is also a problem needs solving.

III. D-S Evidence Theory

The Dempster-Shafer evidence theory is not only a theory of evidence but also that of probable reasoning. It is a framework that can be deployed in diverse areas such as pattern matching, computer vision, expert systems and information retrieval. The D-S evidence theory can handle the randomness and subjective uncertainty together in the trust evaluation. By accumulating evidences, it can narrow down a hypothesis set which provides a powerful method for the representation and process of the trust uncertainty without the demand of prior distribution. Moreover, Dempster's rule of combination is the procedure to aggregate and summarize a corpus of evidence. In the section below, basic concepts in D-S evidence theory are reviewed and will be used to establish model in the proposed method in this paper.

Definition 1. Suppose Φ is a finite set of states, and Φ is defined as a frame of discernment $\{T, \neg T\}$ as the set of propositions under consideration where T and $\neg T$ mean that the given agent considers a given correspondent to be trustworthy or not to be trustworthy, respectively. The number of subsets is 2Φ, and 2Φ is defined as $\{ø, \{T\}, \{\neg T\}, \{T, \neg T\}\}$, where ø represent impossible events while $\{T\}$, $\{\neg T\}$ and $\{T, \neg T\}$ represent trust value, distrust value, and uncertain events respectively.

Definition 2. The mass value of an element A is defined as $m(A)$, and the value of m: 2Φ->[0, 1]. As is closed-world assumption, the mass value of null set is defined as $m(ø)=0$. The basic probability assignment function is defined using the following Eq.(3):

$$\begin{cases} \sum_{A\subseteq\Phi} m(A) = 1 \\ m(\phi) = 0 \end{cases} \tag{3}$$

As is in Definition 1, there has the relationship between $m(\{T\})$, $m(\{\neg T\})$ and $m(\{T, \neg T\})$: $m(\{T\})+m(\{\neg T\})+m(\{T, \neg T\}) = 1$.

Bel: 2Φ->[0, 1] is a belief function over Φ as is defined using the following Eq.(4):

$$Bel(A) = \sum_{B\subseteq A} m(B) \tag{4}$$

Pls: 2Φ->[0, 1] is a plausibility function over Φ as is defined using the following Eq.(5):

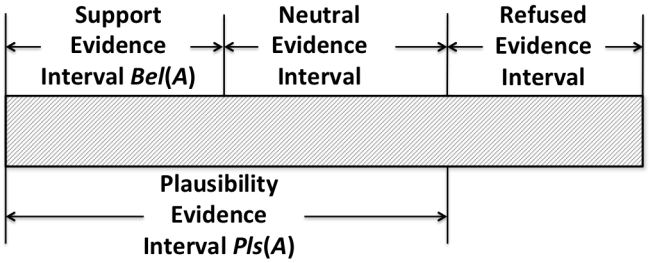


Fig. 5. Evidence interval illustration

$$\begin{cases} Pls(A) = \sum_{B\cap A\neq\phi} m(B) \\ Pls(A) = 1 - Bel(\overline{A}) \end{cases} \tag{5}$$

As is in Definition 1, there are $Bel(\{T\})=m(\{T\})$ and $Pl(\{T\})=m(\{\neg T\})+m(\{T, \neg T\})$.

The relationship between $Bel(A)$ and $Pls(A)$ can be illustrated as the figure in Figure 5.

Definition 3. Dempster's combination rule of two evidences: Suppose Bel_1 and Bel_2 are belief functions over the same frame Φ, with basic probability assignments m_1 and m_2, and focal elements $A_1,...,A_i$, and $B_1,...,B_i$, respectively. Then the function $m(C)$: 2Φ->[0, 1] is defined using the following Eq.(6):

$$\begin{cases} m(C) = m_1(A) \oplus m_2(B) = \dfrac{\sum_{A_i\cap B_j=C} m_1(A_i)m_2(B_j)}{1 - \sum_{A_i\cap B_j=\phi} m_1(A_i)m_2(B_j)} \\ m(\phi) = 0 \end{cases} \tag{6}$$

for all nonempty C, $m(C)$ is a basic probability assignment which describes the combined evidence.

Definiton 4. Dempster's combination rule of more than two evidences: Suppose there are k evidences that are independent with each other over the same frame Φ, with basic probability assignments m_1, m_2, ..., m_p, and focal elements C_1, C_2 and C_p, respectively. Then the function m: 2Φ->[0, 1] is defined using the following Eq.(7):

$$\begin{cases} m(C) = (m_1(C_1) \oplus m_2(C_2) \oplus ...) \oplus m_p(C_p) \\ m(\phi) = 0 \end{cases} \tag{7}$$

for all nonempty C, $m(C)$ is a basic probability assignment which describes the combined evidence.

The trust management strategy proposed in this paper is based on the D-S evidence theory. Firstly, it gives out a formal definition of the trust value. Then it quantifies the direct trust value with a basic confidence function. The direct trust value is used to decide whether a neighbour node is benevolent one. The indirect trust value comes from the

recommendation neighbour node. D-S combination rule is used to combine the indirect trust value together. Then, the combined trust value is compared with the predefined threshold to decide whether there is a cooperative black hole attack.

IV. Proposed Models and Algorithms

A. Proposed NNOM and DTV

As is in the previous work, it 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 a neighbour node is a malicious node or not.

From a time period [T_n, T_{n+1}], each node i will count the recent trust evidence of its neighbour node j. The trust evidence is refreshed form time T_n to T_{n+1} using the following Eq. (8) to Eq. (10). The refresh weight θ is decided by newly counted trust evidence using following Eq. (11). In order to prevent the camouflage and deception, lower θ_1 is used to lower the effect of the evidence supporting benevolent. In order to diminish the effect of malicious actions, a high value is given to θ_2. For the gay hole nodes, when it acts normal behaviour again after malicious actions, the value of θ is set to be θ_3. The value of θ_1, θ_2 and θ_3 is $0 < \theta_3 < \theta_1 < 0.5 < \theta_2 < 1$.

$$\alpha_{n+1} = (1-\theta)\alpha_n + \theta\Delta\alpha \tag{8}$$

$$\beta_{n+1} = (1-\theta)\beta_n + \theta\Delta\beta \tag{9}$$

$$\gamma_{n+1} = (1-\theta)\gamma_n + \theta\Delta\gamma \tag{10}$$

$$\theta = \begin{cases} \theta_1, & if \quad \Delta\alpha \geq \Delta\beta \\ \theta_2, & if \quad \Delta\alpha < \Delta\beta \\ \theta_3, & if \quad \Delta\alpha \geq \Delta\beta \quad then \quad \Delta\alpha < \Delta\beta \end{cases} \tag{11}$$

where:

$\Delta\alpha$: the number of the normal behaviours in [T_n, T_{n+1}];
$\Delta\beta$: the number of the malicious behaviours in [T_n, T_{n+1}];
$\Delta\gamma$: the number of the suspicious behaviours in [T_n, T_{n+1}];

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. (11)
Step 4: Calculate the trust evidence $(\alpha_{n+1}, \beta_{n+1}, \gamma_{n+1})$ at T_{n+1} using Eq. (8)-(10)
Step 5: Calculate the DTV of node j using Eq. (12)-(15)
Step 6: if $B_{ij} - M_{ij} > \eta_1$ and $S_{ij} < \varepsilon_1$
node j is trusted
else if $B_{ij} - M_{ij} < \eta_2$ and $S_{ij} < \varepsilon_1$
node j is malicious node and put into MT.
else
node j is listed on ST
End.

MT stands for the malicious table. ST represents the suspicious table. The value of η_1, η_2 and ε_1 will be studied in the algorithm simulation.

α_n: the trust evidence of normal behaviour at T_n;
β_n: the trust evidence of malicious behaviour at T_n;
γ_n: the trust evidence of suspicious behaviour at T_n;
θ: the refresh weight.

Based on the trust evidence that cares about the historical data, DTV is calculated using following Eq. (12) to Eq. (15):

$$B_{i,j} = \frac{\alpha_n}{\alpha_n + \beta_n + \gamma_n} \tag{12}$$

$$M_{i,j} = \frac{\beta_n}{\alpha_n + \beta_n + \gamma_n} \tag{13}$$

$$S_{i,j} = \frac{\gamma_n}{\alpha_n + \beta_n + \gamma_n} \tag{14}$$

$$D_{i,j} = (B_{i,j}, M_{i,j}, S_{i,j}) \tag{15}$$

where:

$B_{i,j}$: the benevolent actions DTV of node j at T_n;
$M_{i,j}$: the malicious actions DTV of node j at T_n;
$S_{i,j}$: 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

Although there is the proposed DTV, the route through one neighbour node is never set up directly when it is trusted by the observe nodes. As is shown in figure 6, 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

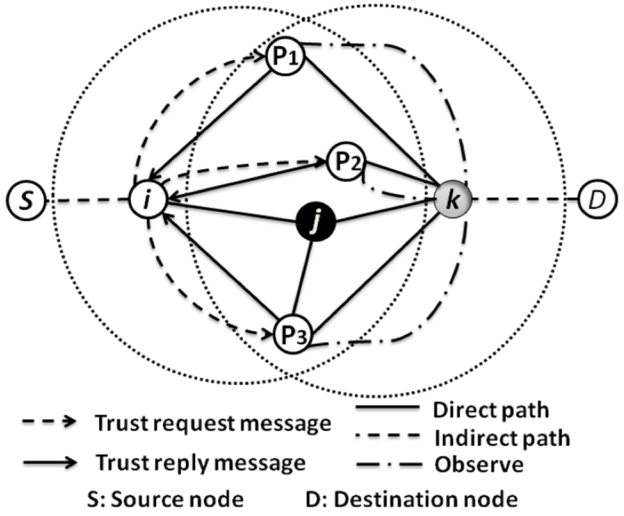


Fig. 6. Neighbour recommendation trust model (NRTM)

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 is cooperative black hole attack or not.

The evaluation difference based on the data distance [13], which means each two data's difference, is calculated by following Eq. (16) to Eq. (17). The evaluation difference of each part in DTV is represented as d_B^p, d_M^p while the range is [0,1] and smaller difference makes them closer to 0.

$$d_B^P = \frac{\sum_{p,q\in N_i, p\neq j, q\neq p} \sqrt{\left|B_{i,q}B_{q,k} - B_{i,p}B_{p,k}\right|}}{\left|N_i\right| - 2} \tag{16}$$

$$d_M^P = \frac{\sum_{p,q\in N_i, p\neq j, q\neq p} \sqrt{\left|M_{i,q}M_{q,k} - M_{i,p}M_{p,k}\right|}}{\left|N_i\right| - 2} \tag{17}$$

where:

d_B^p : the evaluation difference of *B* in DTV;
d_M^p : the evaluation difference of *M* in DTV;
N_i : 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. (18) to Eq. (21):

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 *j*
Step 3: Calculate the evaluation difference using Eq. (16)-(17)
Step 4: Calculate the ITVs of node *j* using Eq. (18)-(21)
Setp 5: Combine different ITVs using Eq. (22)-(25)
Step 6: 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.

MT stands for the malicious table. ST represents the suspicious table. The value of δ_1, δ_2 and ε_2 will be studied in the algorithm simulation.

$$b_{i,k}^p = B_{p,k}\left(1 - \frac{d_B^p}{Max\sqrt{\left|B_{i,q}B_{q,k} - B_{i,p}B_{p,k}\right|}}\right) \tag{18}$$

$$m_{i,k}^p = M_{p,k}\left(1 - \frac{d_M^p}{Max\sqrt{\left|M_{i,q}M_{q,k} - M_{i,p}M_{p,k}\right|}}\right) \tag{19}$$

$$s_{i,k}^p = 1 - b_{i,k}^p - m_{i,k}^p \tag{20}$$

$$I_{i,k}^p = (b_{i,k}^p, m_{i,k}^p, s_{i,k}^p) \tag{21}$$

where:

$b_{i,k}^p$: the benevolent actions ITV of node *k* through node *p* at present T_n;
$m_{i,k}^p$: the malicious actions ITV of node *k* through node *p* at present T_n;
$s_{i,k}^p$: the suspicious actions ITV of node *k* through node *p* at present T_n;
$I_{i,k}^p$: the ITV of node *k* through node *p* at present T_n.

According to the Dempster's combination rule of more than two evidences, the ITVs are combined together to calculate a combined ITV and the ITV is calculated using the following Eq.(22) to Eq.(25):

$$b_{i,k} = b_{i,k}^1 \oplus b_{i,k}^2 \oplus b_{i,k}^3 \oplus \cdots \oplus b_{i,k}^p \tag{22}$$

$$m_{i,k} = m_{i,k}^1 \oplus m_{i,k}^2 \oplus m_{i,k}^3 \oplus \cdots \oplus m_{i,k}^p \tag{23}$$

$$s_{i,k} = s_{i,k}^1 \oplus s_{i,k}^2 \oplus s_{i,k}^3 \oplus \cdots \oplus s_{i,k}^p \tag{24}$$

$$I_{i,k} = (b_{i,k}, m_{i,k}, s_{i,k}) \tag{25}$$

where:

$b_{i,k}$: the benevolent actions ITV of node *k* at present T_n;
$m_{i,k}$: the malicious actions ITV of node *k* at present T_n;
$s_{i,k}$: the suspicious actions ITV of node *k* at present T_n;
$I_{i,k}$: the ITV of node *k* at present T_n.

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

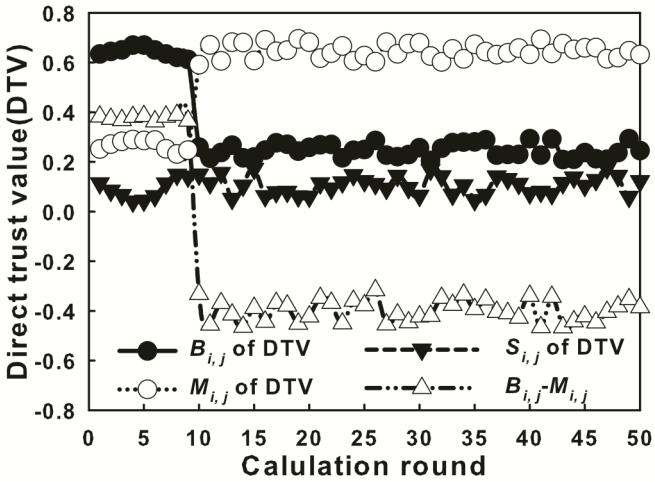


Fig. 7. Transition of DTV on black hole nodes.

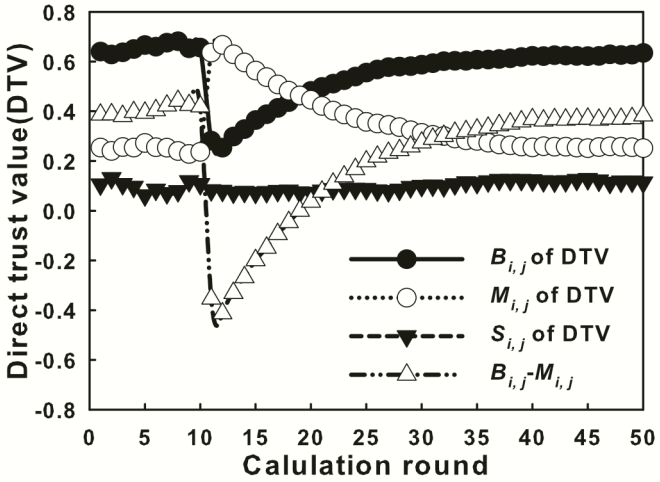


Fig. 8. Transition of DTV on gray hole nodes.

node establishes the route though node *j* and node *k*. If not, node *k* is stored in the MT as a malicious node.

V. Numerical Evaluation

Performance evaluation is firstly conducted to study the proposed DTV and ITV from the aspect of numerical analysis. Matlab is used as the analyser tool. For DTV algorithm, α_0=1, β_0=1 and γ_0=1 are set at initial phase. The historical evidence is given a high weight by assign a low value to θ_1=0.4, a high value to θ_2=0.9 to punish the nodes taking malicious action, and a punish value to θ_3=0.1. In each time period [T_n, T_{n+1}], a set of evaluation evidences is given for three kinds of nodes: normal nodes, black hole nodes, gray hole nodes.

1) For each normal node, a random function is exploited to generate a random number *B* with the probability between [0.6, 0.7] to represent its normal action rate. A random number *M* between [0.2, 0.3] is generated to represent its malicious action rate while the last number *S* between [0, 0.2] is left for the uncertain action rate. The relation between *B*, *M* and *S* is *S*=1-*B*-*M*.
2) For each back hole node, a random function is exploited to generate a random number *B* between [0.2, 0.3] to represent its normal action rate. A random number *M* between [0.7, 0.8] is generated to represent its malicious action rate while the last number *S* between [0, 0.2] is left for the uncertain action rate. The relation between *B*, *M* and *S* is also *S*=1-*B*-*M*.
3) For each gray hole node, firstly it acts as a normal node and all the action rates are generated as in 1), while it acts as a black hole node for a certain time and also follow the action rates in 2), then it acts as a normal node again.

For the ITV algorithm, it is supposed that each recommendation node is given a high reputation because they are all supposed to have been trusted. However, their reputations are different values generated randomly.

1) For normal recommendation node, it will observe the two-hop node based on its own observation. The reputation of the node under observation is given as defined in the front according to its behaviours.
2) If a malicious recommendation node is trying to deceive, it scores a low reputation to a normal node same as what is define as a black hole node or gray hole node, while a high reputation to a malicious node.

A. DTV Performance Evaluation

Figure 7 shows the performance of DTV with the black hole node. The black hole node acts as a malicious node from the 11st round until the last 50th round. 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 from 0.6 and is stable at about 0.2, meanwhile, $M_{i,j}$ increases suddenly from 0.3 and finally rests at around 0.7. $B_{i,j}$-$M_{i,j}$ also drops from minus 0.4 to around minus 0.4. Based on the explanation of Figure 7, some key parameters in the decision part of the DTV algorithm can be set as: η_1 and η_2 is around minus 0.5 and minus 0.2, while ε_1 is around 0.3. In this case, the black hole node is very easy to be filtered out.

Figure 8 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. 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 0.4 to minus 0.5 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 on 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 previous explanation of Figure 8, some key parameters in the decision part of the DTV algorithm can be appropriate as follows: η_1 to be around 0.55, η_2 to be around minus 0.3, and ε_1 to be around 0.15. In this case, the gray hole node is very easy to be filtered out.

Based on the numerical analysis of both black hole attack and gray hole attack, the key parameters in the decision part of the DTV algorithm are set to be: η_1=0.55, η_2=-0.25 and ε_1=0.2.

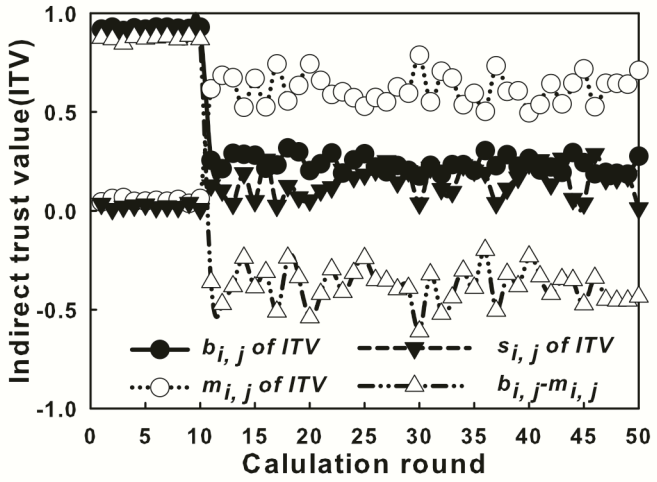


Fig. 9. Transition of ITV on black hole node with 2 benevolent recommenders and 1 deceiving recommender.

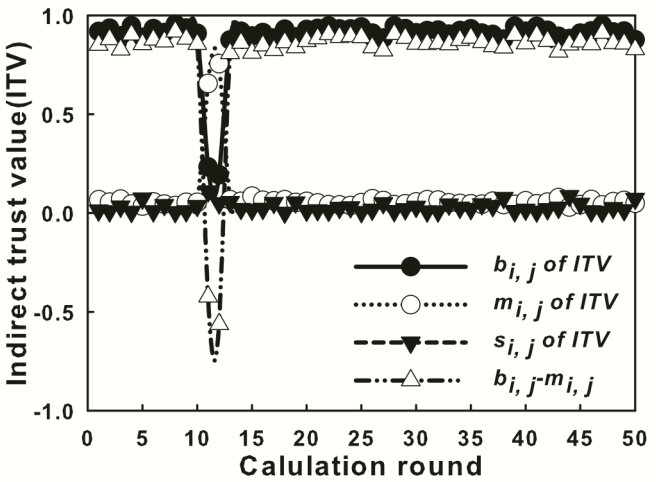


Fig. 10. Transition of ITV on gray hole node with 2 benevolent recommenders and 1 deceiving recommender.

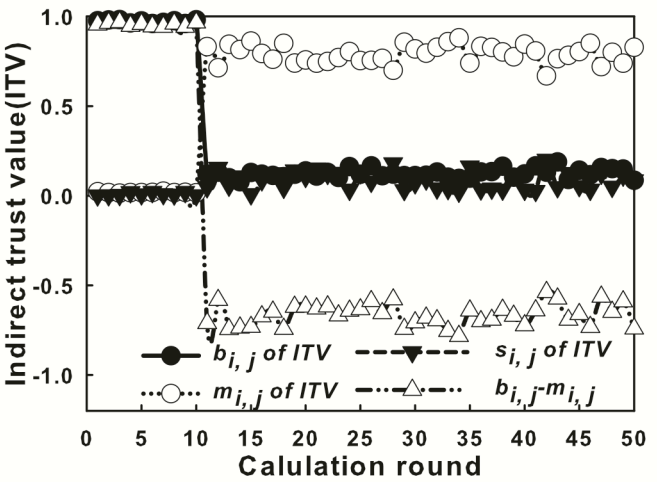


Fig. 11. Transition of ITV on black hole node with 3 benevolent recommenders and 1 deceiving recommender.

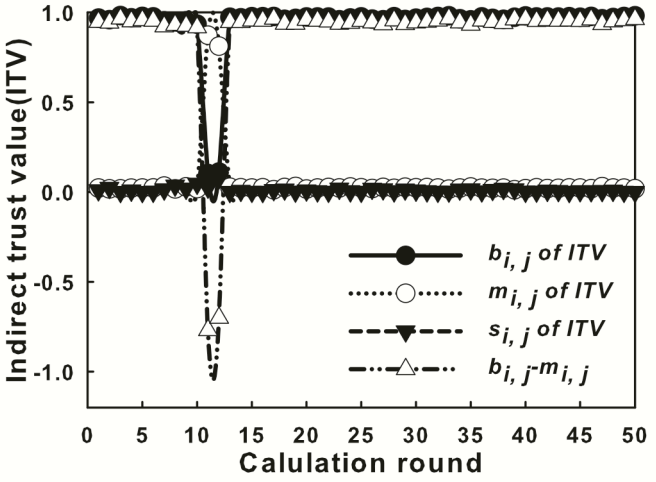


Fig. 12. Transition of ITV on gray hole node with 3 benevolent recommenders and 1 deceiving recommender.

B. ITV Performance Evaluation

Figure 9 shows the performances of ITV influenced by the deceiving nodes under black hole node. For the proposed ITV, it is set that there are totally 3 nodes acting as the recommendation nodes, among which 1 node is cheating. The two-hop node takes black hole action from round 11 to the end. 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 decreasing from the level of 0.9 to around 0.2. $m_{i,k}$ increases from 0.05 but always maintains about 0.9. $s_{i,k}$ changes sharply from 0.05 to 0.2, approximately. After the proposed ITV is implemented, although the deceiving node keep on cheating, the values of $b_{i,k}$, $m_{i,k}$, and $s_{i,k}$ change slowing. The enhancement of the false recommended reputation is minimized. Based on the Figure 9, some key parameters are set to be: δ_1 about 0.9, δ_2 around minus 0.5 and ε_2 is around 0.3.

Figure 10 shows the performances of ITV influenced by the deceiving nodes under gray hole node. For the proposed ITV, it is set that there are totally 4 nodes acting as the recommendation nodes and 1 node is cheating among them. From the result, $b_{i,k}$ first changes in a low speed while still no more than 0.8, then it drops sharply when the two-hop takes malicious action. $m_{i,k}$ increases sharply from 0.05 while always maintains more than 0.9. $s_{i,k}$ changes slightly from 0.05 to 0.2, approximately. Under the proposed ITV, although the deceiving node keeps on cheating, the values of $b_{i,k}$, $m_{i,k}$, and $s_{i,k}$ change slowly. The gray hole node 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. It is apparent that $b_{i,j}$ increases sharply to nearly 0.9, while $m_{i,j}$ decreases immediately to nearly 0.05. Meanwhile, $b_{i,j}$-$m_{i,j}$ also drops from 0.9 to minus 0.7 at the same time. Thus, the enhancement of the falsely recommended ITV is minimized. Based on the analysis of Figure 10, some key parameters are set to be: δ_1 is around 0.8, δ_2 is around minus 0.5 and ε_2 is around 0.1.

Figure 11 and figure 12 are the performances of ITV influenced by deceiving nodes under black hole and gray hole, respectively. Same as what is analysed in figure 9 and figure 10, it is easy to find key parameters to be set. In Figure 11, key parameters are set to be: δ_1 is around 0.9, δ_2 is around minus 0.5 and ε_2 is around 0.25. In Figure 12, δ_1 is around 0.9, δ_2 is around minus 0.5 and ε_2 is around 0.25.

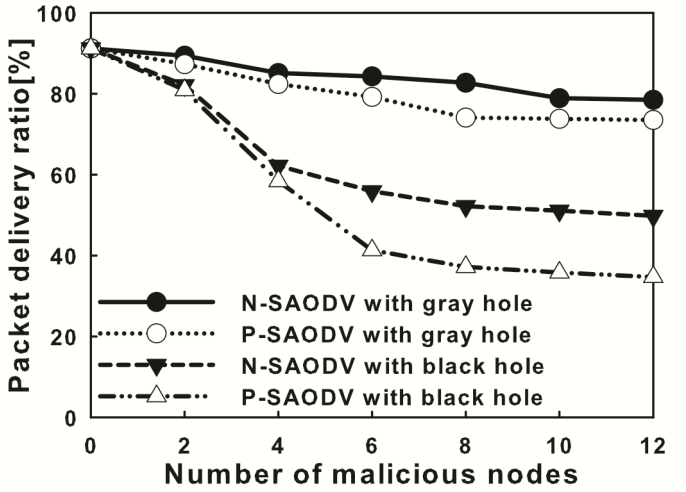


Fig. 13. Packet delivery ratio with single-attack malicious nodes.

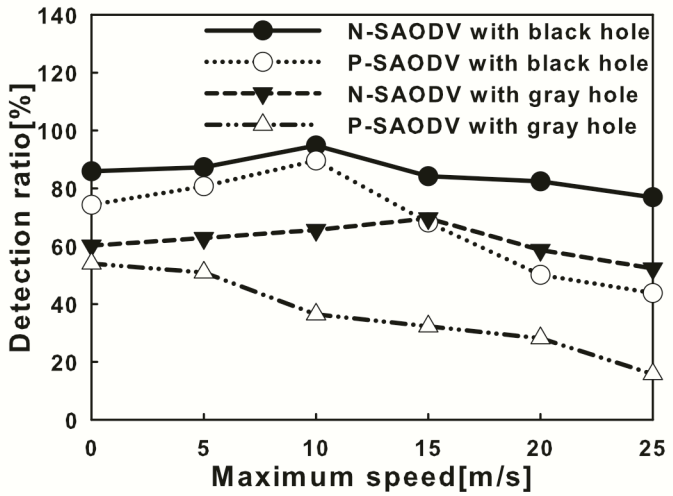


Fig. 14. Packet delivery ratio with single-attack malicious nodes.

Based on the numerical analysis of both black hole attack and gray hole attack, some key parameters in the decision part of the ITV algorithm are set to be: δ_1=0.7, δ_2=-0.3 and ε_2=0.35.

VI. Network Simulation Evaluation

As a second evaluation, the proposed mechanism is implemented in AODV using simulator GloMoSim2.03 to study the packet delivery ratio and detection rate. The parameters are set as in Table 3.

A. Single Attack Performance Evaluation

Figure 13 shows the packet delivery ratio with single-attack black hole node or gray hole node. P-SAODV stands for the AODV protocol with the security mechanism in the previous work. N-SAODV stands for the newly proposed method in this paper. The packet delivery ratio decreases with the increase of the number of malicious nodes in the network. Newly proposed SAOVE detection mechanism will increase the packet delivery ratio more than that of the previous work, in both cases of black hole node and gray hole node. What's more, the black hole case, packet delivery rate decreases more sharply than that in the gray hole case, for the reason that black hole node takes action persistently while gray hole node takes action selectively. Figure 14 shows the detection ratio of P-SAODV and N-SAODV with single-attack black hole node or gray hole node. The detection ratio firstly increases with the increase of the maximum speed of each node, but then it decrease, which is caused by the increase of the packets dropping between nodes. Form these two aspects, it is easy to find that new method shows better performance compared with previous one.

TABLE 3
Simulation Parameters

Parameters	Setting
Simulator	GloMoSim2.03
Routing protocol	P-SAODV／N-SAODV
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	10s
Simulation time	1000s
Mobility model	Random waypoint

B. Cooperative Attack Performance Evaluation

Figure 15 shows the packet delivery rate with cooperative attack malicious nodes. The packet delivery ratio decreases with the increase of the number of malicious nodes in the network. Newly proposed SAOVE detection mechanism will increase the packet delivery ratio more than that of the previous work, in both cases of black hole node and gray hole node. Figure 16 shows the detection ratio of P-SAODV and N-SAODV with cooperative-attack black hole node or gray hole node. The detection ratio firstly increases slightly with the increase of the maximum speed of each node, but then it decrease. The strategy can also reduce the impact from the deceiving neighbour nodes and take advantages of the recommended reputation to make the detection determination more rationally. Form the two aspects, it is easy to find that new method shows better performance compared with the previous one. However, compared with the single-attack, the cooperative-attack is harder to detect even with the new method.

VII. 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. If there is no such recommendation node or

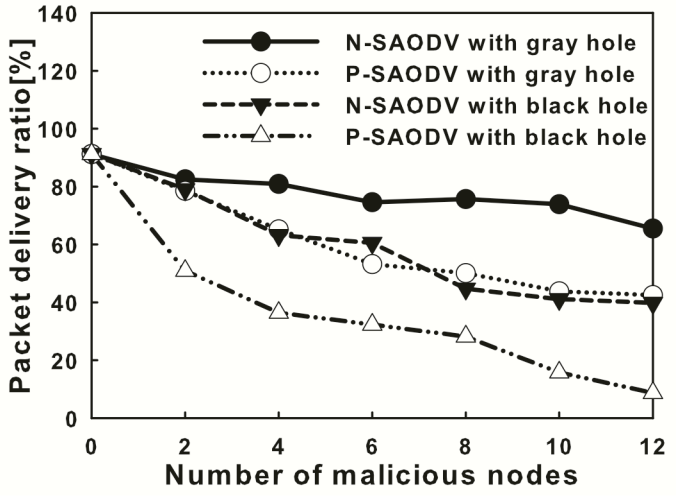


Fig. 15. Packet delivery ratio with cooperative-attack malicious nodes.

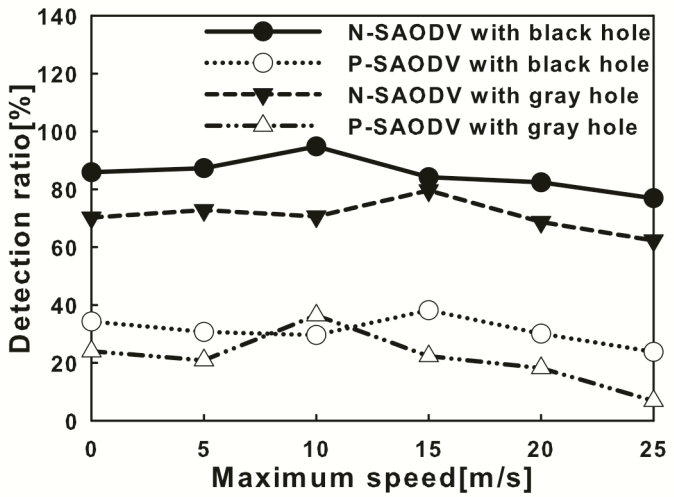


Fig. 16. Detection ratio with cooperative-attack malicious nodes.

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. Some other problems such as energy should also 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. 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 Commun. 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," Comput. and Commun. 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.

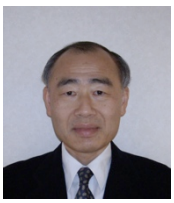
[9] H. Chen, "Task-based trust management for wireless sensor network," Int. J. of Security and Its Applications SERSC, vol. 3, No. 2, April 2009.

[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.

Bo Yang received his B. E. degree in computer science and technology from Xi Dian University, Xi'an, China, in 2009. He received his second B.E. degree in economics from Xi'an Jiaotong University, China, 2012. Currently, he is working toward the M.E. degree in the Global Information and Telecommunication Studies, Waseda University, Tokyo, Japan. He won the ICACT best paper award in Feb. 2012. His present research emphasizes on the study of security problems in the wireless networks, such as ad hoc networks, MANETs, WSNs etc.

Ryo Yamamoto received his B.E. and M.E. degree in electronic information systems from Shibaura Institute of Technology, Tokyo, Japan, in 2007 and 2009. He is presently a research associate of Global Information and Telecommunication Institute, Waseda University. He received the IEICE young researcher's award in 2010. His current research interests are mobile ad hoc networks and cross-layered protocols.



Yoshiaki Tanaka received the B.E., M.E., and D.E. degrees in electrical engineering from the University of Tokyo, Tokyo, Japan, in 1974, 1976, and 1979, respectively. He became a staff at Department of Electrical Engineering, the University of Tokyo, in 1979, and has been engaged in teaching and researching in the fields of telecommunication networks, switching systems, and network security. He was a guest professor at Department of Communication Systems, Lund Institute of Technology, Sweden, from 1986 to 1987. He was also a visiting researcher at Institute for Posts and Telecommunications Policy, from 1988 to 1991, and at Institute for Monetary and Economic Studies, Bank of Japan, from 1994 to 1996. He is presently a professor at Global Information and Telecommunication Institute, Waseda University, and a visiting professor at National Institute of Informatics. He received the IEEE Outstanding Student Award in 1977, the Niwa Memorial Prize in 1980, the IEICE Achievement Award in 1980, the Okawa Publication Prize in 1994, the TAF Telecom System Technology Award in 1995 and in 2006, the IEICE Information Network Research Award in 1996, in 2001, in 2004, and in 2006, the IEICE Communications Society Activity Testimonial in 1997 and in 1998, the IEICE Switching System Research Award in 2001, the IEICE Best Paper Award in 2005, the IEICE Network System Research Award in 2006, in 2008, and in 2011, the IEICE Communications Society Activity Award in 2008, the Commendation by Minister for Internal Affairs and Communications in 2009, and the APNOMS Best Paper Award in 2009. He is a Fellow of IEICE.