A Threshold-Adaptive Reputation System on Mobile Ad Hoc Networks

SUMMARY In recent years, huge potential benefits from novel applications in mobile ad hoc networks (MANET) have been discussed extensively. However, without robust security mechanisms and systems to provide safety shell through the MANET infrastructure, MANET applications can be vulnerable and hammered by malicious attackers easily. In order to detect misbehaved message routing and identify malicious attackers in MANET, schemes based on reputation concept have shown their advantages in this area in terms of good scalability and simple threshold-based detection strategy. We observed that previous reputation schemes generally use predefined thresholds which do not take into account the effect of behavior dynamics between nodes in a period of time. In this paper, we propose a Threshold-Adaptive Reputation System (TARS) to overcome the shortcomings of static threshold strategy and improve the overall MANET performance under misbehaved routing attack. A fuzzy-based inference engine is introduced to evaluate the trustiness of a node’s one-hop neighbors. Malicious nodes whose trust values are lower than the adaptive threshold, will be detected and filtered out by their honest neighbors during trustiness evaluation process. The results of network simulation show that the TARS outperforms other compared schemes under security attacks in most cases and at the same time reduces the decrease of total packet delivery ratio by 67% in comparison with MANET without reputation system.

key words: mobile ad hoc network, network security, reputation system, fuzzy logic

1. Introduction

A mobile ad hoc network (MANET) is a wireless communication network formed by a collection of mobile nodes. In MANET, nodes can join and leave the network anytime and instantly establish communication without any fixed infrastructure. MANET has been targeted by a wide range of applications such as disaster relief, military communication in battle fields and vehicle-to-vehicle communications in roadway.

1.1 Background and Motivation

In MANET, the transmission range of mobile nodes is limited by the battery power of each node and protocol specification. Therefore, when a source node wants to establish a connection with its destination node that is multi-hops away, the intermediate nodes between the source and destination node must act as routers and cooperatively relay the data through network. Since the message data is relayed between nodes, it is possible that a malicious intermediate node could modify data packets or drop packets during relay process. To overcome this security threat, schemes based on reputation credibility with simple threshold-based detection strategy have become one of the most promising solutions in the past few years [1]–[5].

In general, a reputation system with proper threshold value can effectively detect malicious routing behaviors in MANET. However, it is difficult to determine the proper threshold of the reputation system due to the dynamic nature of MANET topology. In addition, a reputation system with static threshold value may make a wrong judgment to a neighbor node. From our literature review, the thresholds of reputation systems in previous research works are all static values. This motivated us to design the Threshold-Adaptive Reputation System (TARS) to overcome the shortcomings of static threshold strategy and improve the overall MANET performance under misbehaved routing attack. A fuzzy-based inference engine is introduced to evaluate the trust of a node’s one-hop neighbors based on their trust values. Malicious nodes will be detected and filtered out during this evaluation process.

1.2 Related Work

In recent years, secure schemes on MANET to address the selfish and/or misbehaved nodes by enforcing node cooperation. These techniques can be widely classified into three categories: credit-based schemes, reputation-based schemes and acknowledgment-based schemes.

1.2.1 Credit-Based Schemes

The idea of credit-based schemes is to give a node incentive to provide its valuable resources and service other nodes in MANET. In order to create incentives, the mechanism of virtual currency with payment system needs to be designed and implemented on a node.

Buttyan and Hubaux [6] proposed the packet purse model and packet trade model in their paper. In packet purse model, the data sender that needs the forwarding service must append some nuglets (virtual currency) to the packet before sending the corresponding packet. Each intermedia-
turns off

A forbidden concept is adopted in PCOM. When a node

to join the network and share the resources from other nodes.

allow nodes who have not cooperated with other nodes yet,

(PCOM). Similar to the incentive concept, PCOM does not

this misbehavior called Proactive COoperation Mechanism

cept of this work is that each node in the network monitors

posed a predictive security model for MANET. The con-

transmission range. The idea of activity-based overhearing

observer node monitors all nodes residing in its wireless

based overhearing, instead only observing its next hop, an

watchdog module to extend the detection ability. In activity-

proposed the activity-based overhearing technique based on

pass through these misbehaved nodes. In [9], Kargl et al.

modules of the observer exclude the existing routes that

outgoing packets of its next hop and detects whether the next

hop forwards its received packets. If the packet drop rate of

the observed nodes exceeds a given threshold, the pathrater

modules of the observer exclude the existing routes that

pass through these misbehaved nodes. In [9], Kargl et al.

proposed the activity-based overhearing technique based on

watchdog module to extend the detection ability. In activity-

based overhearing, instead only observing its next hop, an

observer node monitors all nodes residing in its wireless

transmission range. The idea of activity-based overhearing

is inherited by many solutions [2], [10]–[12].

Newly proposed reputation-based schemes [11], [13],

[15] apply fuzzy inference system to evaluate the trustiness

of a node in MANET. Alampalayam and Kumar [11] pro-

posed a predictive security model for MANET. The con-

cept of this work is that each node in the network monitors

the network parameters. If the network parameters change

rapidly, there may be an attack occurred. Manickam and

Shanmugavel [13] proposed a fuzzy-based trusted routing

protocol based on AODV [14]. In this research, each node

verifies the trust value of its neighbors using fuzzy inference

technique. Nodes will interact only with the trusted neigh-

bors. Wang and Huang [15] applied fuzzy logic to select the

routing path. The route selection of this scheme considers

node reputation, bandwidth and hop count of the candidate

route at the same time.

1.2.3 Acknowledgment-Based Schemes

The main concept of acknowledgment-based schemes is to
detect the selfish and misbehaved nodes by verifying

whether the destination node received the transmitted pack-

tets.

In [16], Awerbuch et al. described a probing mecha-
nism to detect the selfish node. Each destination node must

send corresponding acknowledgment packet (ACK) back to

the source node when it received a data packet. If the num-

ber of ACK packet losses violates the acceptable threshold

in a route, the source node starts a binary Probing to search

where packets are being dropped. Kargl et al. [9] proposed

an enhanced solution called iterative probing. In iterative

probing, each probing command addresses to one node. The

probing command in data packet contains one encrypted

node identity. If a data packet does not include any probing

command, then the probing field of this packet will con-

tain a random number. This mechanism prevents packet re-

cipients from distinguishing the probing packets among

received data packets. Therefore, the malicious nodes cannot

circumvent the probing. Recently, Liu et al. [17] proposed

the 2ACK scheme to detect the malicious nodes. The basic

idea of 2ACK scheme is to check the reception status of next

two hops in the route. Each node in the route observes the

next hop by checking whether the destination of next-hop

node in the route received the data packet from next hop. If

the destination of next hop received the data, it will send the

ACK packet to previous two hops. Therefore, the node in a

route can detect whether the next hop indeed sends the data

packets.

1.3 Challenging Issues

Based on reviews in Sect. 1.2, we observed that the credit-
based schemes usually require embedded tamper-proof

hardware and system setups to secure credit payment pro-

cess, while it is not an easy task in distributed MANET en-

vironment. Acknowledgment-based schemes can reduce the

false positive ratio by verifying the reception status of data

packets. However, they can only detect the packet dropping

attack. Therefore, acknowledgment-based schemes must as-

sociate with other misbehavior detection techniques to rein-

force the network security in MANET.

Reputation-based schemes do not require tamper-proof

hardware and they detect malicious nodes in a specific net-
rules to be setup in advance for different types of network environments and attacks. This scheme is not easily scalable in MANET. On the contrary, our proposed scheme can dynamically construct the fuzzy sets and membership functions under all kinds of network environments. In [13], [15], the authors first performed MANET simulation experiments to identify the suitable system parameters and manually configured them in their fuzzy inference systems later. Instead of requiring data training process, our system automatically configures system parameters at run time. This adaptive characteristic makes the system performance of our scheme better than other schemes. More comparisons of our proposed system and other types of reputation system are discussed in Sect. 4.

The rest of this paper is organized as follows. We describe our system models in Sect. 2. Threshold-adaptive reputation system is introduced in Sect. 3. In Sect. 4, network simulation is performed to evaluate the performance of proposed scheme. Finally, we remark our conclusions and future work in Sect. 5.

2. System Models and Assumptions

In this section, we describe the network model of MANET and the attack model on MANET environment with their corresponding assumptions before introducing our new approach – Threshold-adaptive Reputation System.

2.1 Network Model

We assume each node in a MANET equipped with IEEE 802.11-compatible wireless communication device which features the promiscuous mode configuration. In network layer, all nodes adopting the Ad hoc On-demand Distance Vector (AODV) routing protocol [14] is assumed. In AODV, when a source node wants to send packets to a destination, if it does not has the route to the destined node in its routing table, the source node will broadcast the route request message (RREQ) to its neighbor nodes. If the neighbors received the RREQ message and some of them have routes established to the destination, they will send route replay messages (RREP) back to the source node directly to inform the source node a route is found. Otherwise, neighbor nodes will forward the RREQ messages to other nodes in the network. When the source node receives the RREP message from its neighbors, the source node will establish the shortest route based on routing information in its routing table and start to send the data packets to the destination node.

2.2 Attack Model

The aim of an attacker in the network is to disrupt network communications or decrease network performance. When a malicious node received a RREQ message or RREP message, instead normally increasing the hop count field by one in the message header and forwarding this message if necessary, the attacker arbitrarily change its responding behavior provisioned by routing protocol by decreasing the value of hop count field before it transmits the message to the next hop. This kind of malicious behavior can generate false information to nodes such that an illusion of shorter route for communication connections is created. In consequence, more data traffic will be directed and passed through the malicious node. A malicious node can also decrease the network performance easily by randomly dropping incoming data packets.

The ultimate goal of proposed scheme is to correctly detect these type of security threats and isolate these identified malicious nodes from the rest of nodes in MANET.

3. Threshold-Adaptive Reputation System

In this section, we introduce a new network security scheme called Threshold-Adaptive Reputation System (TARS) for MANET environment. TARS can be implemented and installed on each node in MANET such that every legitimate node becomes an observer and can evaluate the trustiness of
Its neighbor nodes. A credit-broken neighbor node will be isolated by the observer as a malicious attacker in the network.

3.1 Scheme Overview

The system architecture of TARS scheme is shown in Fig. 1. Each node equipped with the TARS will monitor the inbound and outbound packets of its neighbor nodes through the behavior observation module. A behavior reasoning module based on fuzzy inference technique is built to calculate the trust value of each observed neighbor node, which indicates the level of trustiness from the observer point of view. In order to compute the trust value of an observed node, the behavior reasoning module requires predefined rule set for fuzzy inference process along with the input of observation data from the behavior observation module. The rule repository module is designed to store the predefined fuzzy logic rules. All computed trust values are automatically stored in the trust manager module before further processing. The trust manager evaluates the trustiness of observed nodes by comparing their corresponding trust values with the isolation threshold. In general, a neighbor node is identified as a malicious attacker if its trust value is below the isolation threshold, which indicates the relative plausibility of derived reputation credit (trust value) to the observer and is set by the observer based on current network environment. Once a misbehaved node is identified, the misbehavior isolation module is invoked by the trust manager to disrupt existing communication routes and forbidden new route establishment through the observer to the malicious node. A trust sharing module is also introduced in this architecture to distribute the stored trust values owned by an observer node to other nodes it trusts in MANET. In the following, we describe these TARS modules in detail.

3.2 Behavior Observation

A node installed with the TARS is capable of acting as an observer. An observer can utilize its behavior observation module to monitor the inbound and outbound packets of its neighbor nodes and record the behavior status of each observing neighbor. In practical, packet monitoring is done by implementing promiscuous mode functionality in network interface. If a neighbor node does not follow the routing protocol when processing a received packet or not forward the packet that needs to be sent, the identity of this malicious node and its misbehavior will be recorded in the misbehavior table of observer’s TARS system. The misbehavior table is used to record the first-hand observation. In general, an entry in misbehavior table contains the node identity $i$, the misbehavior ratio to RREQ packet forwarding $Q_i$, the misbehavior ratio to RREP packet forwarding $P_i$, and the misbehavior ratio to data packet forwarding $D_i$. The misbehavior ratio of a neighbor node is defined as the number of suspected misbehaviors to the number of total observed behaviors. Depending on the definition and requirement of misbehavior detection, various metrics of misbehavior measurement can be applied to the behavior observation module. It is easy to insert new observing items into or delete existing measurement items from the misbehavior table.

3.3 Rule Repository

Since TARS utilizes fuzzy inference technique to dynamically derive the trustiness for each neighbor node of the observer in a predefined period of time regularly, a set of inference rules must be set in advance based on the predefined fuzzy sets and membership functions of input and output parameters, respectively, where the input parameters are the metrics of misbehavior measurement depicted in Sect. 3.2 and the output parameter indicates the trust value of a neighbor node. The rule repository module is designed to store the inference rule set for behavior reasoning module to query. An example of fuzzy inference rule set is shown in Table 1.

3.4 Behavior Reasoning

The objective of behavior reasoning module is to generate an adaptive (or relative) trust value for each observed node. In order to catch the influential and dynamic factors in MANET for behavior indication, the technique of Fuzzy Inference System (FIS), is adopted to build the engine of behavior reasoning module.

In behavior reasoning module, three sets of membership functions are predefined for corresponding input parameters of the FIS, which are the $Q_i$, $P_i$, and $D_i$ obtained from the misbehavior table in behavior observation module.

### Table 1: Inference rules in rule repository module.

<table>
<thead>
<tr>
<th>Input parameters</th>
<th>Output</th>
<th>Input parameters</th>
<th>Output</th>
<th>Input parameters</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Q_i$</td>
<td>$P_i$</td>
<td>$D_i$</td>
<td>$Q_i$</td>
<td>$P_i$</td>
<td>$D_i$</td>
</tr>
<tr>
<td>L</td>
<td>L</td>
<td>VH(1)</td>
<td>M</td>
<td>L</td>
<td>VH(0.8)</td>
</tr>
<tr>
<td>L</td>
<td>L</td>
<td>M</td>
<td>H(1)</td>
<td>M</td>
<td>L</td>
</tr>
<tr>
<td>L</td>
<td>L</td>
<td>H</td>
<td>M(1)</td>
<td>M</td>
<td>L</td>
</tr>
<tr>
<td>L</td>
<td>M</td>
<td>L</td>
<td>M(0.5)</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>L</td>
<td>M</td>
<td>M</td>
<td>L(0.5)</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>L</td>
<td>M</td>
<td>H</td>
<td>L(1)</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>L</td>
<td>H</td>
<td>L</td>
<td>L(0.5)</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>L</td>
<td>H</td>
<td>H</td>
<td>L(0.8)</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>L</td>
<td>H</td>
<td>H</td>
<td>VL(1)</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

**Fig. 1** The system architecture of threshold-adaptive reputation system scheme.
For each input parameter, three linguistic variables defined as “Low”, “Medium” and “High” are used as the qualified input values. Each linguistic variable represents a fuzzy set that is uniquely defined by a membership function. As each input parameter of the FIS has three possible linguistic states, the corresponding membership function set contains three membership functions, respectively. In general, the selection of membership function requires expert knowledge. However, with the advantage of low computational overhead and easy to use, triangular functions have been extensively used in fuzzy systems for wireless networks [11], [13], [18], [19]. In this paper, triangular function is chosen as the membership function of inference engine. The fuzzy sets and membership functions of input parameters are shown in Fig. 2 in which three corresponding membership functions, respectively. In general, the selection of membership function requires expert knowledge.

In Fig. 2(a), $A_0$ indicates the overlapping area between two fuzzy sets defined by the corresponding membership functions of linguistic variables “Low” and “Medium”. $Q_{MAX}$ and $Q_{MIN}$ indicate the maximum and minimum values of misbehavior ratio to RREQ packet forwarding in the misbehavior table, respectively. The behavior difference, $D_b$, in terms of misbehavior ratio to RREQ packet forwarding between all observed nodes is calculated as $D_b = Q_{MAX} - Q_{MIN}$. The crossing point of membership functions “Low” and “Medium”, $a$, can be derived as $a = \frac{D_b}{2} + Q_{MIN}$. The centroid of the fuzzy set of linguistic variable “Medium”, $b$, is computed as $b = \frac{D_b}{2} + Q_{MIN}$. The crossing point of membership functions “Medium” and “High”, $c$, is set as $c = \frac{D_b}{2} + Q_{MIN}$. The fuzzy sets and membership functions of other input parameters, $P_i$ and $D_i$, are constructed and calculated in the same way. Note that when behavior reasoning module constructs the fuzzy set of $D_i$, our system only gathers the values of misbehavior ratio to data packet forwarding in misbehavior table which are larger than the nature packet drop ratio $R_{nat}$. This action is to filter out the similar effect caused by the nature packet drop ratio; as nodes move out of the packet transmission range between itself and the next hop destination, the transmitting packet will be naturally dropped. Our scheme does not consider the impact of nature packet drop ratio on other input parameters because the process of route discovery in MANET only takes very short amount of time. In such case, the effect of nature drop ratio of control packets (e.g., RREQ and RREP packets) due to node movement is very limited and can be ignored to reduce computational overhead without influencing the evaluation capability of proposed fuzzy system module. On the other hand, a data transmission session takes much longer period of time in usual, normal node movement could significantly affect the nature packet drop ratio. In consequence, the effect of nature drop ratio of data packets could not be ignored. In terms of the output parameter in our FIS, the trust value is described using five linguistic variables “Very Low”, “Low”, “Medium”, “High”, and “Very High”. The range of the trust value is between zero and one (i.e., $T_{MIN} = 0$ and $T_{MAX} = 1$). The range of five fuzzy sets and corresponding membership functions of the trust value (output parameter) are both shown in Fig. 3.

In this FIS module, there are three input parameters and each of them has three fuzzy sets. Therefore, there are $3^3$ inference rules to be defined and stored in the rule repository. The rules are used when the FIS module infers the trust value. The design of fuzzy inference rules is based on the analysis of the network and expert knowledge. In addition, all rules can be modified dynamically before the invocation of inference process. This flexible characteristic of FIS module allows the proposed TARS system to utilize the knowledge of experts and fine tune the reasoning engine (i.e., to apply different membership function) under different network environments. The rules are realized in the form of “IF-THEN” format and aggregated with fuzzy operator “AND”. For example, the first rule in Table 1 can be interpreted as follows:

IF (the misbehavior ratio to RREQ packet forwarding is “Low”) AND the misbehavior ratio to RREP packet forwarding is “Low”) THEN (the trust value is “Very High”). This rule is certainly true. Therefore, the expert (or rule designer) weighted this rule by 1.

Deffuzzification is the last step in behavior reasoning. This step is to convert the output of inference rules into the crisp trust value. In this paper, the behavior reasoning mod-

---

Fig. 2 The fuzzy sets and membership functions of input parameters in behavior reasoning module: (a) misbehavior ratio to RREQ packet forwarding (b) misbehavior ratio to RREP packet forwarding (c) misbehavior ratio to data packet forwarding.

Fig. 3 The fuzzy sets and membership functions of output parameter (i.e., the adaptive trust value) in behavior reasoning module.

tio to data packet forwarding in misbehavior table which are larger than the nature packet drop ratio $R_{nat}$. This action is to filter out the similar effect caused by the nature packet drop ratio; as nodes move out of the packet transmission range between itself and the next hop destination, the transmitting packet will be naturally dropped. Our scheme does not consider the impact of nature packet drop ratio on other input parameters because the process of route discovery in MANET only takes very short amount of time. In such case, the effect of nature drop ratio of control packets (e.g., RREQ and RREP packets) due to node movement is very limited and can be ignored to reduce computational overhead without influencing the evaluation capability of proposed fuzzy system module. On the other hand, a data transmission session takes much longer period of time in usual, normal node movement could significantly affect the nature packet drop ratio. In consequence, the effect of nature drop ratio of data packets could not be ignored. In terms of the output parameter in our FIS, the trust value is described using five linguistic variables “Very Low”, “Low”, “Medium”, “High”, and “Very High”. The range of the trust value is between zero and one (i.e., $T_{MIN} = 0$ and $T_{MAX} = 1$). The range of five fuzzy sets and corresponding membership functions of the trust value (output parameter) are both shown in Fig. 3.

In this FIS module, there are three input parameters and each of them has three fuzzy sets. Therefore, there are $3^3$ inference rules to be defined and stored in the rule repository. The rules are used when the FIS module infers the trust value. The design of fuzzy inference rules is based on the analysis of the network and expert knowledge. In addition, all rules can be modified dynamically before the invocation of inference process. This flexible characteristic of FIS module allows the proposed TARS system to utilize the knowledge of experts and fine tune the reasoning engine (i.e., to apply different membership function) under different network environments. The rules are realized in the form of “IF-THEN” format and aggregated with fuzzy operator “AND”. For example, the first rule in Table 1 can be interpreted as follows:

IF (the misbehavior ratio to RREQ packet forwarding is “Low”) AND the misbehavior ratio to RREP packet forwarding is “Low”) THEN (the trust value is “Very High”). This rule is certainly true. Therefore, the expert (or rule designer) weighted this rule by 1.

Deffuzzification is the last step in behavior reasoning. This step is to convert the output of inference rules into the crisp trust value. In this paper, the behavior reasoning mod-

---

Fig. 2 The fuzzy sets and membership functions of input parameters in behavior reasoning module: (a) misbehavior ratio to RREQ packet forwarding (b) misbehavior ratio to RREP packet forwarding (c) misbehavior ratio to data packet forwarding.
ule performs the conversion and gets the crisp trust value by calculating the centroid of area (or center of gravity) formed by the aggregated membership function of output parameter, which is one of the most popular defuzzification methods used in FIS. The computation formula for centroid of area is listed in Eq. (1), where $y_j$ represents the centroid of each output membership function, $\mu_i(y)$ indicates the membership of trust, $T^*$ is the output of crisp trust value and $M$ represents the number of output membership functions. In this example, $M = 5$. In brief, for each observed node $i$, the behavior reasoning module of the observer node will compute its corresponding trust value $T_i = T^*$, based on the embedded FIS engine, predefined inference rules, linguistic variables and selected membership functions.

$$ T^* = \frac{\sum_{j=1}^{M} \mu_i(y_j) \cdot y_j}{\sum_{j=1}^{M} \mu_i(y_j)} $$

### 3.5 Trust Manager

Trust manager module in TARS performs trustiness evaluation to all targeted neighbor nodes. In addition, all derived trust values of targeted neighbors and the value of isolation threshold, $T_{ih}$, are stored in the trust manager module. A neighbor node is identified as a malicious node after trustiness evaluation is performed, if the corresponding trust value is below the isolation threshold of observer and the corresponding drop ratio of data packets is larger than nature packet drop ratio, $R_{nd}$. Note that the isolation threshold is acted as the measurement tool of relative plausibility of trustiness to nodes being evaluated. Therefore, it is logically adaptive through the evaluation of adaptive trust values of neighbor nodes to decide the acceptable level of trustiness under current network environment and the behavior difference among neighbor nodes. In other words, under different conditions, the same value of isolation threshold indicates different trustiness levels.

### 3.6 Trust Sharing

Trust sharing module is designed for occasions when sharing trust values set among legitimate nodes is required, such as supporting tracing feature for historical trust values of an identified misbehaved node. In order to distribute the trust information with low communication overhead, the trust sharing module can piggyback the trust values set in control packets. In AODV routing protocol, HELLO packet can be used for a legitimate node to broadcast its trust values set to its legitimate neighbors.

A shared trust value of node $i$, denoted as $T_{ih}$, received from a neighbor node can also serve as the extra observation information to the hosting observer. The behavior reasoning module can adopt the shared information and its corresponding effect easily. As an example shown in Eq. (2), the trust value of node $i$, $T_i$, for the hosting observer is computed with a predefined weight for received trust value $\alpha$, $T_{ih}$ and $T_{ic}$ which is the current trust value of node $i$ stored in the trust manager module.

$$ T_i = (1 - \alpha) T_{ic} + \alpha T_{ih} $$

### 3.7 Misbehavior Isolation

The module of misbehavior isolation in TARS designates to execute the isolation strategy upon the identified misbehaved neighbor nodes. Since TARS is a module-oriented system, various isolation strategies can be implemented on misbehavior isolation module and nodes with TARS can select different isolation strategy based on its own demand or positioned network environment. The isolation strategy we adopted here is to store the identity of misbehaved node into the blacklist of this module with a timestamp, and send route error control packets (RERR) to the source node to reestablish a new route without misbehaved node. To prevent the identified malicious nodes become intermediate nodes of another route sometime later, the isolation module will check incoming packets and drop those who pass toward nodes in the blacklist. A control parameter for isolation period of time is introduced as an option feature to setup the blocking duration of nodes in the blacklist associated with the stored timestamps. Once the isolation period of a node is expired, its corresponding record is deleted from the blacklist. This feature provides an opportunity for nodes in the blacklist to rejoin the network and communicate with others provided that they will change their network behaviors toward normalization.

### 4. Performance Evaluation

In order to investigate detection performance and precision on malicious nodes and robustness to dynamic MANET environments of proposed TARS scheme, we conducted simulations with network simulator, NS-2 [20], to evaluate the TARS scheme. We implemented TARS scheme on the top of AODV routing protocol. The inference engine from MATLAB Fuzzy Logic Toolbox is modified as the behavior reasoning module of TARS. The simulation environment is constructed with 50 nodes which are randomly placed in a 1500 m × 300 m rectangular field. The mobility pattern is random waypoint model [21]. The pause time parameter is set to 10 seconds in our simulations. The moving speed of a node is uniformly generated between (0, $V_{max}$], where $V_{max}$ is the maximal speed of nodes within the simulation. The communication traffic used is 15 CBR (Constant Bit Rate) connections with randomly selected source-destination node pairs. All the data packets are 512 bytes long and send at a speed of 3 packets per second. The path loss model in physical layer is two-ray ground propagation model. The MAC layer protocol utilizes Distributed Coordination Function (DCF) of the IEEE 802.11 and the link bandwidth is 2M bits/sec. The radio propagation range of each node is
250 meters. The simulation results are averaged over ten runs and each run is executed for 600 seconds in simulation time.

In each simulation run, 20% nodes in the network are randomly selected as malicious nodes. The behaviors of each malicious node are simulated based on the attack model of Sect. 2.2, and the probability for a malicious node to drop a received data packet, $P_d$, is set to 0.5.

In order to compare the effectiveness of proposed adaptive threshold concept with previously published concepts on reputation-based scheme, three mechanisms are evaluated along with TARS. We briefly introduce these three schemes as follows.

The first scheme is an enhanced version of watchdog mechanism [5] with activity-based overhearing feature [9]. If any neighbor node does not forward normal data packets to its next hop nodes, the observer will decrease its corresponding reputation credit. An attacker is identified by an observer when the number of dropping packets exceeds the predefined threshold ($T_{acq}$). The value of $T_{acq}$ is set to 30 in our experiments.

Static threshold-based reputation scheme from [3] is introduced here as the second mechanism. This scheme uses the number of dropping packets per sampling interval to identify a malicious node. If the number of dropping packets per unit interval to an observed node is above predefined threshold value, the system will consider this node as an attacker. We set the static threshold of this scheme as 22 packet drops per 5 seconds in our simulations.

We found that it is not sufficient and precise for a reputation-based scheme to identify a malicious node in a dynamic MANET environment by detecting the number of misbehaved routing actions or the packet drop rate per unit time interval only. Therefore, we propose the third mechanism called acquaintance-based reputation scheme. The concept of this scheme is that an observer node should be acquainted with its observing nodes (i.e., its neighbors) for a period of time before performing any evaluation process. A malicious node is identified when the number of observed behaviors to the targeted node is above the acquaintance threshold $T_{acq}$ and the packet drop ratio of the targeted node is above the packet drop threshold $T_{drop}$ at the same time. We set $T_{acq} = 30$ and $T_{drop} = 0.3$ in our simulations.

For our proposed scheme TARS, the nature packet drop ratio of a node, $R_{ndr}$, is set to 0.25 and the isolation threshold $T_I$ is set to 0.3 in our simulations.

The condition to identify an attacker are different in each scheme. In our proposed system attack identification occurs when trust value of next hop node in a data connection is bellowing to isolation threshold, $T_I = 0.3$. The attack identification occurs in Watchdog scheme is when a neighbor drop more than 30 packets. The attack identification occurs in static threshold-based scheme is when a neighbor drop more than 22 packets in 5 seconds. Finally, the attack identification occurs in acquaintance-based scheme is when it obverse data forwarding of its neighbor more than 30 times and the packet drop ratio is above 0.3.

After attack identification, all schemes in the simulation will isolate this suspicious node by dropping all packets it generates in a predefined system blocking time. We set blocking time as 320 seconds in simulations.

The effectiveness of proposed scheme can be evaluated from the Packet Delivery Ratio (PDR). The packet delivery ratio is defined as the ratio of the total number of data packets received by destinations over the total number of data packets sent by sources. The PDR takes into account both packet drops caused by bad channel conditions and node mobility, and attack from malicious nodes. This metric can reflect performance robustness of proposed scheme.

The detection ability of proposed scheme can be evaluated from Attack Detection Ratio (ADR). The attack detection ratio is defined as the number of successful attack detections over the number of successful attacks that are created by malicious nodes. In this paper, successful detection is defined as a node that is identified as an attacker by a security scheme and it is indeed an attacker. Successful attack is defined as an attacker successfully becomes an intermediate node in a route and starts to drop incoming data packets.

We apply false positive ratio to evaluate the detection accuracy in various schemes. The false positive ratio is defined as the number of claimed detection events in which the suspicious node actually is not an attacker to the number of total detection events.

### 4.1 Packet Delivery Ratio

In Fig. 4 the comparison of six schemes on the performance of packet delivery ratio is shown, where the x-axis indicates the maximum moving speed of nodes in simulation and the y-axis indicates the packet delivery ratio of each compared scheme. The symbol of original AODV indicates there is not any malicious node in the network and the symbol of original AODV (under attack) defines there are 20% attackers in the network which is without any security protection scheme available. As the figure shows, if there is no reputation system activated in the network, the network performance in terms of PDR degrades about 15% in low mobility environment and 13% in high mobility environment, respectively. In most cases, the PDR of TARS is outperforming
other compared schemes. However, in low mobility environment PDR of TARS is lower than acquaintance-based scheme. This is because in the low mobility environment the TARS may not be able to collect sufficient behavior actions of participants (nodes) to construct the fuzzy sets which can well represent the current condition of network; therefore, the derived reputation credits for observed nodes are not able to reflect the real situation, neither. In other words, more malicious nodes may not be isolated under this low mobility environment than they should be in normal cases.

4.2 False Positive Ratio

In Fig. 5, the comparison of four schemes on the performance of false positive ratio is shown. The false positive ratio increases with the speed of nodes in MANET. This is because, when the mobility of nodes increases, the frequency of route break increases at the same time and the packet drop rate also increases. A reputation-based scheme in MANET cannot distinguish whether the cause of packet drops is from node mobility or the misbehaviors of nodes in general. This is why for most reputation-based schemes, it is impossible to prevent the false positive detections. In Fig. 4, we can observe that even there is no malicious node in MANET, the packet delivery ratio still decreases with speed. In some cases, the natural packet drop ratio due to mobility may exceed the static threshold of detection scheme. This is why the false positive ratios of static threshold-based scheme and watchdog scheme are very high. The TARS outperforms other schemes in false positive ratio because it does not use the concept of static threshold to identify possible attacks. Instead, TARS collects the parameters in MANET, dynamically constructs the target fuzzy set and evaluates them with its decision engine. When the data drop ratio becomes higher in all nodes, the defined linguistic variables of fuzzy sets, “Low”, “Medium” and “High” along with corresponding membership functions, will dynamically reflect the current environment in TARS. This context-aware feature in TARS makes attack detection more accurate than other schemes.

4.3 Attack Detection Ratio

The comparison of attack detection ability under various node mobility to four schemes is shown in Fig. 6. The attack detection ratio exceeds 1 in watchdog scheme. This is because we applied activity-based overhearing technique in watchdog scheme which extends attack detection and attacker identification to all nodes within the transmission range of the observer. On the other hand, TARS makes attacker identification only to its next hop neighbor in a route. Therefore, the attack detection ratio of TARS is lower than activity-based reputation system. The acquaintance-based scheme needs to observe sufficient amount of node behaviors before making a judgment of attack occurrence. Therefore, the attack detection ratio of acquaintance-based scheme is much lower than watchdog scheme with activity-based overhearing.

In Fig. 6, we found there is an interesting phenomenon in which the attack detection ratio of TARS increases with the speed of nodes in MANET. This is because, when node mobility increases, the behavior observation module can get more chances to collect more misbehavior actions from more different network participants (nodes). More entries in misbehavior table the fuzzy sets construction and behavior reasoning can be more objective. This is similar to the real world; if we known more people, we can differentiate who is honest and who is deceitful more easily.

In practice, it is hard to define the number of packet drops per time interval without any statistical analysis. Therefore, the attack detection ratio of static threshold-based scheme is very low in Fig. 6. The low detection ratio of static reputation-based scheme also affects its packet delivery ratio in Fig. 4. The packet delivery ratio of static reputation-based scheme is only higher than original AODV (under attack) 1%. This result manifests that the design of dynamic threshold reputation system is indispensable in MANET.
5. Conclusion

In MANET, misbehaved routing attack from malicious nodes is still a serious security problem even though various detection schemes were done for recent years. By conducting detailed review and investigation, we notice that it is very difficult for a reputation-based detection scheme to determine the suitable threshold value by which malicious nodes can be distinguished from honest nodes. By following this practical need, we proposed a new type of reputation-based scheme called threshold-adaptive reputation system (TARS) which can derive adaptive trust value for each neighbor it observes and make the judgment of trustiness level semantically to each observed node. Fuzzy-based inference technique is adopted in TARS to perform the calculation of trust values. Network simulator is utilized to perform experiments on proposed TARS scheme. The simulation results show that our proposed system can defend against misbehaved routing nodes and improve the network performance with low false positive ratio when network is under attack. In comparison with other schemes under security attacks, the TARS outperforms them in most cases in terms of packet delivery ratio and false positive ratio. Since the mechanism of reputation judgment in our system is derived adaptively based on current network environment, this scheme can be easily deployed to all kinds of MANET environments.

In our system we observed that the attack detection ratio to misbehaved node is low when there are few attackers or nodes are in low mobility status. We think that our scheme can combine with the activity-based overhearing technique to increase the attack detection ratio of our reputation system. On the other hand, how to isolate malicious nodes more efficiently and quickly in dynamic MANET environment is required for further study.

Acknowledgments

The authors gratefully acknowledge the support from Taiwan Information Security Center (TWISC) projects and partial support from general research projects, which are all sponsored by the National Science Council, Taiwan, under the Grants No. NSC 97-2219-E-001-001, NSC 97-2219-E-011-006, NSC 96-2221-E-011-148-MY2 and NSC 97-2218-E-011-014.

References

Hsiao-Chien Tsai was born on September 21, 1981, in Taoyuan County, Taiwan. He received his B.S. degree in information management from the National Yunlin University of Science and Technology, Yunlin, Taiwan, in 2005, and the M.S. degree in information management from the National Taiwan University of Science and Technology, Taipei, Taiwan in 2007. He is currently a Ph.D. candidate of Information Management at the National Taiwan University of Science and Technology. His research interests include mobile ad hoc network applications and security, network protocol design, and pervasive computing.

Nai-Wei Lo was born on October 29, 1966, in Kaohsiung City, Taiwan. He received his B.S. degree in engineering science from the National Cheng-Kung University, Tainan, Taiwan, in 1988, and the M.S. and Ph.D. degrees in computer science and electrical engineering from the State University of New York at Stony Brook, NY, in 1992 and 1998, respectively. He is currently an assistant professor of Department of Information Management at the National Taiwan University of Science and Technology, and a member of the IEEE communications society. His research interests include RFID applications and security, wireless network routing and security, Web technology, and fault tolerance.

Tzong-Chen Wu was born on September 24, 1960, in Kaohsiung County, Taiwan. He received the B.S. degree in the Department of Information Engineering from National Taiwan University (Taiwan) in 1983, the M.S. degree in the Department of Applied Mathematics from National Chung Hsing University (Taiwan) in 1989, and the Ph.D. in the Department of Computer Science and Information Engineering from National Chiao Tung University (Taiwan) in 1992. From August 1992 to January 1997, he has been the associate professor at the Department of Information Management, National Taiwan University of Science and Technology (NTUST, Taiwan Tech.). Since February 1997, he has been the professor at the Department of Information Management of NTUST, and chaired the Department of Information Management from 1999 to 2003. He is the members of IEEE, ACM, and the Chinese Cryptology and Information Security Association (CCISA). His research interests include cryptography, data security, network security, and data engineering. During his academic carrier, Professor Wu has published more than 70 journal papers and more than 70 conference papers related to the topics of cryptology and information security. Now, he serves as the Dean of School of Management of NTUST, President of CCISA, and the Director of Taiwan Information Security Center at NTUST (TWISC@NTUST).