# A Cooperative Trust Bit-Map Routing Protocol Using the GA Algorithm for Reducing the Damages from the InTs in WANETs

Hsing-Chung Chen[1,2*] and Hui-Kai Su[3]
[1]Dept. of Computer Science and Information Engineering
Asia University, Taichung 41354, Taiwan, R.O.C.
cdma2000@asia.edu.tw
[2]Dept. of Medical Research, China Medical University Hospital
China Medical University Taichung, 40402, Taiwan, R.O.C. (Research Consultant)
[3]Dept. of Electrical Engineering
National Formosa University, Yunlin 632, Taiwan, R.O.C.
hksu@nfu.edu.tw

**Abstract**

The wireless ad hoc network (WANET) is a type of wireless network in which some nodes are decentralized as well as self-organized in a wireless local area network. In recent years, insider threats increasingly damage the works not only in computer information systems, but also many wireless communications systems e.g. WANETs. We must take into consideration that the majority of insider threats come from users who are fully authorized to use the WANET systems they are accessing. Due to these kinds of situations, a Cooperative Trust Bit-Map Routing Protocol (CTBRP) using an $n$-Bits Cooperative Trust Bit-Map Routing Table ($n$-CTBRT) is proposed to be used against insider threats in WANETs. This CTBRP proposes using a Generic Algorithm in this paper for establishing cooperative evaluating trust values. Each node evaluates her/his neighboring nodes in order to reduce the untrusted routes. Thus, it could reduce the damage away from the insider threats in a WANET. This approach is one of behavioral-based techniques. In fact, the compromised nodes or selfish nodes or non-honest nodes will be evaluated as having low trust values or scores. Once a relay node had been compromised or damaged by insider threats in this WANET, the communication system will use this approach to find out about it according to its abnormal behaviors. Therefore, the proposed routing protocol in the WANET could evaluate the wrongful behaviors of the compromised node or a selfish node efficiently in order to prevent InTs.

**Keywords**: cooperative routing protocol, trust routing protocol, wireless ad hoc network

## 1 Introduction

A wireless ad hoc network (WANET) is a type of wireless network in which some nodes are self-organized in a wireless local area network [16, 14, 3]. In recent years, many researchers are [16, 14, 15, 7, 6] focusing on either trust-based routing algorithms for improving the networking security and relative performances. The primary purposes in security are to identify the potential attacks, threats, and vulnerabilities of WANET systems [9, 10]. In general, threats in the WANET can be classified as either passive or active [9, 10]. Some passive attacks do not disrupt the operations of an WANET communications system, but attempt to learn information about WANET communications by eavesdropping [9, 10]. Although difficult to detect, some passive attacks cause less damage if well designed confidentiality mechanisms are adopted [2, 8]. In addition, some active threats could be further divided into outside

*Journal of Internet Services and Information Security (JISIS)*, volume: 4, number: 4 (November 2014), pp. 52-70
*Corresponding author: Department of Computer Science and Information Engineering, Asia University, Taichung Country, Taiwan 41354, Fax, +886-4-23305737

threats and insider threats (InTs). Some outside threats are launched by attackers who are not equipped with the main key materials in a WANET communications system, while InTs are those from compromised nodes that hold the main key materials. In fact, most insider threats are actually the work of people with authorized access to WANET communications systems or information, not hackers. Consider the that the majority of insider threats come from users who are fully authorized to use the systems they are accessing [11]. Because of the fact that cyber security can do little to stop them, it is very difficult to detect malicious uses by the authorized users. Compared to the outside threats, the InTs obviously cause more serious damage to WANETs.

The concepts from the domain of Trusted Computing [12, 9, 10, 5] can be applied to the example of WANETs in order to establish extended trust capabilities between mobile devices. The communications between directly connected mobile devices of WANETs are protected by cryptographic protocols making use of trusted mechanisms that serve as the guardian on mobile devices. Furthermore, some attempts [3, 4, 2, 8] have been also proposed for adapting to the particular circumstances mentioned above. For instance, two proposed routing protocols in [3, 4] designed the event-driving or role-based routing protocols for more flexibility in adapting to the particular circumstances. In their schemes [3, 4, 2, 8], each node will periodically broadcast a "hello message" in order to discover neighboring nodes. They also need a border node acting as a knowledge discovery (KD) agent [3, 4, 2, 8] for each event or role. It is used to deliver the network topology messages, and then gather the reply information in order to collect the $n$-bits map routing table ($n$-BMRT) [3, 4, 2, 8]]. There are not only the conventional and power-aware routing protocols, but also the protocols [16, 14, 3, 15, 7, 4, 2, 8] that are mainly focused on the hop number, power consumption or traffic of a route, respectively. They did not consider the issue of how to practically evaluate the trust values for trust bit-map routing in order to reduce the damage for InTs in a WANET. In order to cope with these factors at the same time, a Trust-Based Cooperation Bit-Map Routing Protocol (TCBRP) was proposed by H.-C. Chen et al in [5] using an $n$-bits Trust-Based Cooperation Bit-Map Routing Table ($n$-TCBRT) in the WANETs. The main contribution in [5] is the first investigation of the $n$-Bits map routing protocol using trust-based cooperative cross-layer technology, which copes with not only mobility, power consumption and real traffic, but also trust evaluation on the maintained routes.

However, the detection of InTs have to use not only technicalities in cryptographic protocols but also behavioral-based techniques. The research works [12, 9, 10, 5] mentioned above could not fully support the InTs in WANETS. Therefore, a Cooperative Trust Bit-Map Routing Protocol (CTBRP for short, hereafter) using an $n$-Bits Cooperative Trust Bit-Map Routing Table ($n$-CTBRT) is also proposed in this paper for ensuring the trusted routing table is in order to reduce the damage from the InTs in WANETs. Specifically, the Generic Algorithm is employed in this paper for cooperatively evaluating trust scores. Therefore, the malicious nodes or selfish nodes or non-honest nodes will be evaluated to show their low scores in the trust values in the WANET communication system.

The remainder of this paper is organized as follows: In section 2, we introduce the related works. In section 3, we first present the cooperative trust route selection based on the genetic algorithm. Then, the discussions and security analyses are described in section 4. Finally, we draw our conclusions in section 5.

## 2 Related Works

In this section, the traditional GA Algorithm is described as below.

## 2.1 GA Algorithm

Genetic Algorithms (GAs) [1, 13] are the computational approaches that play a critical role in the emerging new branch of biology known as functional genomics [1]. GAs were first proposed by Holland [1] and more recently reviewed and enhanced by Goldberg [1]. A GA maintains a population of candidate solutions for the problem at hand, and makes it evolve by iteratively applying a set of stochastic operations consisting of selection operation, recombination operation and mutation operation [13]. Selection replicates the most successful solutions found in a population at a rate proportional to their relative quality [13]. Recombination decomposes two distinct solutions and then randomly mixes their parts to form novel solutions [13]. Mutation randomly perturbs a candidate solution [13]. An example of a simple GA [13] is described as below. A flow chart of a *simple GA procedure* is presented s below as well as shown in Fig. 1.

Step 1: Produce an initial population of individuals;
Step 2: Evaluate the fitness of all individuals;
Step 3: **while** *(termination condition not met)* **do**
  S3.1: Select appropriate individuals for reproduction;
  S3.2: Crossover operation between individuals;
  S3.3: Mutate individuals;
  S3.4: Evaluate the fitness of the modified individuals;
  S3.5: Generate a new population;
**end**
Step 4: End;

**Algorithm 1:** Simple GA Procedure

## 2.2 Review of Trust-Based Cooperation Bit-Map Routing Protocol

The Trust-Based Cooperation Bit-Map Routing Protocol (TCBRP) using an $n$-bits Trust-Based Cooperation Bit-Map Routing Table ($n$-TCBRT, for short) for Ad Hoc Networks was proposed in [5]. It assumed that there are $m$ nodes, collected to a set denoted as $N = \{N_1, N_2, ..., N_m\}$, number of $N$ is noted as $m = |N|$, in a WANET. Within the $m$ nodes there are some nodes acting as border nodes, where the border node $N_{Br} \in N$ have enough power and computing ability. It is the node which could generate an $n$-TCBRT.

Each node will broadcast the "hello packet" to its neighbors in a specific signal range. For instance, node $N_j \in N$ broadcasts the hello packet, in which the format is shown as Fig 2, to node $N_j \in N, j \neq i$. When node $N_j$ receives the hello packet, it will measure its signal strength $Rx_{i,j}$. The node $N_j$ will also do the calculations via *Procedure 1* [5] as seen below.

**Procedure 1:**

**Step 1:** The reception node $N_j$ calculates the reception rate $RR_j$ and transmission rate $TR_j$ on the current sampling time $t_k$.

**Step 2:** The reception node $N_j$ calculates the cooperative factors $E_{i,j}^{1st}, E_{i,j}^{2nd}, E_{i,j}^{3rd}, ..., E_{i,j}^{l-th}$, which are dependent on the limitation of the topology. The cooperative factors [5] are calculated as seen fig. 3.

where $p_i$ is the node $N_i$'s remaining power, $p_i^{max}$ is the node $N_i$'s initial power, $TH_h, h \in \{1, 2, 3, ..., l\}$ is the threshold value dependent on the transmission distances. The *cooperative condition function* $f_c(\bullet)$

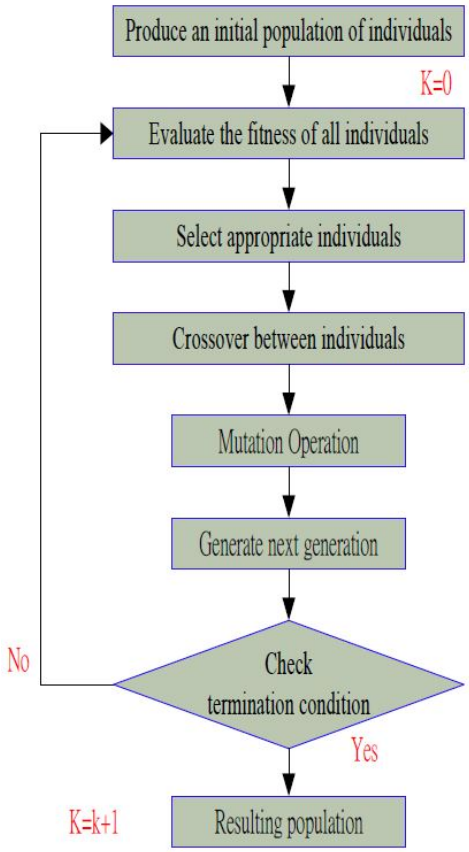


Figure 1: Flow chart of simple GA procedure.

| Type | Hello Packet |
|---|---|
| Node IP address | 224.0.2.0~224.0.255.255 |
| Node Mac address | 00.00.00.00.00.00.00 ~FF.FF.FF.FF.FF.FF |
| Sequence number | 00000001 |
| Life time | 100 (Mini Seconds) |

Figure 2: An example of hello packet format[5].

[5] is defined in the equation (1) as below.

$$f_c(Rx_{i,j}, RR_j, TR_j, p_i, p_j, p_i^{max}, p_j^{max}) = Rx_{i,j} \times \frac{TR_j}{RR_j} \times \frac{p_i}{p_i^{max}} \times \frac{p_j}{p_j^{max}} \quad (1)$$

**Step 3:** The reception node $N_j$ will broadcast the 'reply packet' as shown in Fig. 4 to the sender node $N_i$

$$E_{i,j}^{1-st} = \begin{cases} 1, \ if \ f_c\left(Rx_{i,j}, RR_j, TR_j, p_i, p_j, p_i^{max}, p_j^{max}\right) \geq TH_1 \\ 0, \ if \ f_c\left(Rx_{i,j}, RR_j, TR_j, p_i, p_j, p_i^{max}, p_j^{max}\right) < TH_1 \end{cases},$$

$$E_{i,j}^{2-nd} = \begin{cases} 1, \ if \ TH_1 \leq f_c\left(Rx_{i,j}, RR_j, TR_j, p_i, p_j, p_i^{max}, p_j^{max}\right) \geq TH_2 \\ 0, \ if \ f_c\left(Rx_{i,j}, RR_j, TR_j, p_i, p_j, p_i^{max}, p_j^{max}\right) < TH_2 \end{cases},$$

$$E_{i,j}^{3-rd} = \begin{cases} 1, \ if \ TH_2 \leq f_c\left(Rx_{i,j}, RR_j, TR_j, p_i, p_j, p_i^{max}, p_j^{max}\right) \geq TH_3 \\ 0, \ if \ f_c\left(Rx_{i,j}, RR_j, TR_j, p_i, p_j, p_i^{max}, p_j^{max}\right) < TH_3 \end{cases},$$

$$\bullet$$
$$\bullet$$
$$\bullet$$

$$E_{i,j}^{l-th} = \begin{cases} 1, \ if \ TH_{l-1} \leq f_c\left(Rx_{i,j}, RR_j, TR_j, p_i, p_j, p_i^{max}, p_j^{max}\right) \geq TH_l \\ 0, \ if \ f_c\left(Rx_{i,j}, RR_j, TR_j, p_i, p_j, p_i^{max}, p_j^{max}\right) < TH_l \end{cases}.$$

Figure 3: The cooperative factors.

including its neighbors.

| **Type** | **Reply Packet** |
|---|---|
| Node IP address | 224.0.2.0~224.0.255.255 |
| Node Mac address | Ab.cd.ef.12.23.34.45.56 |
| Sequence Number | 00000011 |
| Cooperative factors | $E_{i,j}^{1-st} \,\|\|\, E_{i,j}^{2-nd} \,\|\|\, E_{i,j}^{3-rd} \,\|\| \ldots \|\| \, E_{i,j}^{l-th}$ |
| Trust values | $\tau_{i,j}^{1-st_{(2)}} \,\|\|\, \tau_{i,j}^{2-nd_{(2)}} \,\|\|\, \tau_{i,j}^{3-rd_{(2)}} \,\|\| \ldots \|\| \, \tau_{i,j}^{l-th_{(2)}}$ |

Figure 4: An example of reply packet format.

The node $N_j$ will reply with the 'reply packet', individually, back to node $N_i$ with the format as below, where the symbol "||" denotes the concatenation operator to connect the fixed length of the messages.

**Step 4:** After receiving the reply packet messages from neighboring nodes, the node $N_i$ then generates the neighbor information and gathers them into a cooperative neighbor information table, see Table 1. All nodes are connected under the satisfying cooperative condition $E_{i,j}^{1-st}$ as shown in Fig. 5. After having been broadcasted, all hello packets will be collected by all nodes. Next, a cooperative

neighbor information table (CNI Table) will be generated. An example of a CNI table is shown in Table 1.

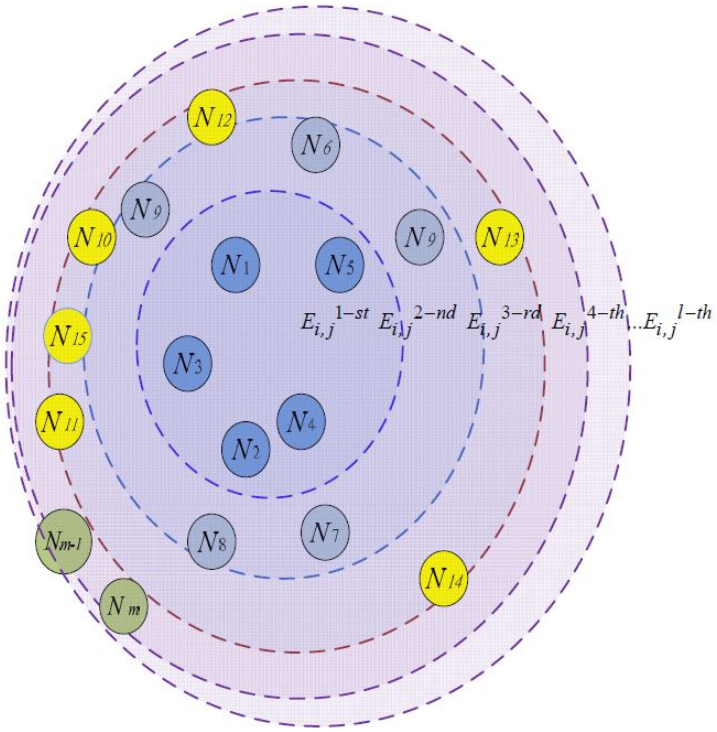


Figure 5: Each node is evaluated in its cooperative condition to determine whether it is satisfying a cooperative evaluation $E_{i,j}^{x-th}, x \in \{1,2,3,4\}$.

Table 1: The neighbors' information table under satisfying cooperative condition for a node $N_k$.

| Node ID | Neighboring nodes | Number of neighboring nodes | Under satisfying cooperative condition | Trust or Reputation Scores (%) |
|---|---|---|---|---|
| $N_k$ | $N_{k-3}, N_k, N_{k+1}$ | 2 | $E_{i,j}^{1st}$ | 80, 70, 85 |
| $N_k$ | $N_{k+3}, N_{k+4}$ | 2 | $E_{i,j}^{2nd}$ | 40, 80 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

**Step 5:** After receiving the cooperative factors $E_{i,j}^{1st}, E_{i,j}^{2nd}, E_{i,j}^{3rd}, ..., E_{i,j}^{l-th}$ in the reply packet sent by node $N_j \in N, j \neq i$, the node $N_i$ will calculate the cooperative scores by equation (2), individually.

$$s_{i,j} = f_s(E_{i,j}^{1st}, E_{i,j}^{2nd}, E_{i,j}^{3rd}, ..., E_{i,j}^{l-th}) \quad (2)$$

where $f_c(\bullet)$ is a type of evolution function.

**Step 6:** Each node is evaluated in its cooperative condition as shown in Fig. 5 to determine whether it is satisfying a cooperative evaluation $E_{i,j}^{x-th}, x \in \{1,2,3,4\}$ after all hello packets having been broadcasted and collected by the border node.

**Step 7:** Node $N_i \in N$ or border node $N_{br} \in N$ also collects the trust cooperative evaluations from other neighboring nodes. Next, the border node $N_{br} \in N$ will generate the $n$-TCBRT as shown in Table 2.

Table 2: The $n$-TCBRT.

| Node ID / Node ID | $N_i$ | $N_j$ | ... | $N_y$ |
|---|---|---|---|---|
| $N_i$ | – | $\left[s^1 s^2 ... s^x ... s^l \,\|\|\, \tau^1 \tau^2 ... \tau^x ... \tau^l\right]$ | ... | $\left[s^1 s^2 ... s^x ... s^l \,\|\|\, \tau^1 \tau^2 ... \tau^x ... \tau^l\right]$ |
| $N_j$ | $\left[s^1 s^2 ... s^x ... s^l \,\|\|\, \tau^1 \tau^2 ... \tau^x ... \tau^l\right]$ | – | ... | $\left[s^1 s^2 ... s^x ... s^l \,\|\|\, \tau^1 \tau^2 ... \tau^x ... \tau^l\right]$ |
| $N_k$ | $\left[s^1 s^2 ... s^x ... s^l \,\|\|\, \tau^1 \tau^2 ... \tau^x ... \tau^l\right]$ | $\left[s^1 s^2 ... s^x ... s^l \,\|\|\, \tau^1 \tau^2 ... \tau^x ... \tau^l\right]$ | – | $\left[s^1 s^2 ... s^x ... s^l \,\|\|\, \tau^1 \tau^2 ... \tau^x ... \tau^l\right]$ |
| $N_l$ | $\left[s^1 s^2 ... s^x ... s^l \,\|\|\, \tau^1 \tau^2 ... \tau^x ... \tau^l\right]$ | $\left[s^1 s^2 ... s^x ... s^l \,\|\|\, \tau^1 \tau^2 ... \tau^x ... \tau^l\right]$ | ... | $\left[s^1 s^2 ... s^x ... s^l \,\|\|\, \tau^1 \tau^2 ... \tau^x ... \tau^l\right]$ |
| . . . | . . . | . . . | . . . | |
| $N_x$ | $\left[s^1 s^2 ... s^x ... s^l \,\|\|\, \tau^1 \tau^2 ... \tau^x ... \tau^l\right]$ | $\left[s^1 s^2 ... s^x ... s^l \,\|\|\, \tau^1 \tau^2 ... \tau^x ... \tau^l\right]$ | | $\left[s^1 s^2 ... s^x ... s^l \,\|\|\, \tau^1 \tau^2 ... \tau^x ... \tau^l\right]$ |
| $N_y$ | $\left[s^1 s^2 ... s^x ... s^l \,\|\|\, \tau^1 \tau^2 ... \tau^x ... \tau^l\right]$ | $\left[s^1 s^2 ... s^x ... s^l \,\|\|\, \tau^1 \tau^2 ... \tau^x ... \tau^l\right]$ | ... | – |

*where* $\tau^1 \tau^2 ... \tau^x ... \tau^l = 11...1...1$ *in initial trust phase, and* $n = 2l$ *(bits).*

# 3 Cooperative Trust Route Selecting Based On the Genetic Algorithm

In this section, we formulate the network model, the trust evaluation model, as well as the evolution function using the GA approach in order to establish an integrating trusted platform for the WANET in cyberspace.

## 3.1 Network Model

A typical WANET consists of a trust agent (TA) and a large number of nodes which are randomly deployed at a certain interest area within cyberspace. It assumes that there are $m$ nodes plus a TA node named as $N_{TA}$ in a WANET, all part of a collected set denoted as $N = \{N_1, N_2, ..., N_m\} \cup \{N_{TA}\}$. The

number of $N$ is noted as $|N| = m+1$. Each node $N_i \in N$ is stationary in a location. For differentiation purposes, each node has a unique nonzero identifier which is assumed in this paper. Moreover, the communication is bidirectional in which two nodes within their wireless transmission range (TR) may communicate with each other. The TA node, is a trustable and powerful device. It has sufficient computational and storage capabilities and is responsible for the reputation computing of all participating nodes, maintaining the trust evaluations, and updating the trust-based bit-map table to defend malicious or untrusted insider threats from some compromised nodes. The example initial state of topology in cyberspace is shown as Fig. 6.

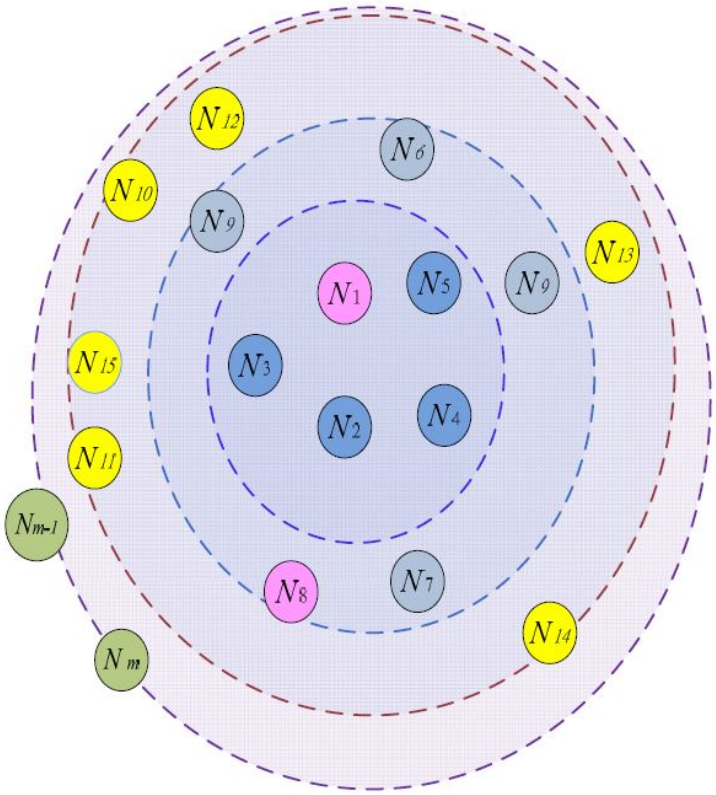


Figure 6: Initial state of topology in cyberspace.

## 3.2 Trust Evaluation Model

When a source node $N_i \in N$ intends to send the data packet to the destination node $N_j \in N$, it will select immediate nodes which have the highest cooperative score and trust value with lowest cost routing path. After finding all immediate nodes $\{N_k | N_k \in [N_i \leftrightarrow N_j]\}$ belonging to the routing path $[N_i \leftrightarrow N_j]$ as shown in equation (3) according to the initial $n$-TCBRT, the node will send the data packet to the destination node via some immediate selected nodes. Procedure 2 [5] will ensure that the immediate node truly forwards the data packet after receiving it from the source node, and also judge whether the neighbor is selfish or unselfish.

$$[N_i \leftrightarrow N_j] = [N_i \leftrightarrow N_{i+1} \parallel N_{i+1} \leftrightarrow N_{i+2} \parallel \ldots \parallel N_{j-1} \leftrightarrow N_j] \tag{3}$$

where $(N_i \leftrightarrow N_{i+1})$ is the starting path, $(N_{j-1} \leftrightarrow N_j)$ is the target path, $(N_{i+x} \leftrightarrow N_{i+x+1})$ is an intermediate path except starting path and target path.

**Procedure 2:**

**Step 1:** After receiving the data packet from a source node $N_i$, the immediate node $N_k$ will deliver the data packet to the next best immediate node and reply with an acknowledgement packet which the format refers to in Fig. 4. $N_i$ The node and the previous immediate node will perform the trust evolution function [5], output the new trust values $\tau_{i,j}^{1st} \| \tau_{i,j}^{2nd} \| \tau_{i,j}^{3rd} \| \ldots \| \tau_{i,j}^{l-th}$, and gather them into her/his neighbor evolution information table, as shown in Table 3.

Table 3: The Updated $n$-TCBRT.

| Node ID \ Node ID | $N_i$ | $N_j$ | ... | $N_y$ |
|---|---|---|---|---|
| $N_i$ | $\left[11\ldots1\ldots1 \| 11\ldots1\ldots1\right]_{i,i}$ | $\left[s^1 s^2 \ldots s^x \ldots s^l \,\|\| \tau^1 \tau^2 \ldots \tau^x \ldots \tau^l\right]_{i,j}$ | ... | $\left[s^1 s^2 \ldots s^x \ldots s^l \,\|\| \tau^1 \tau^2 \ldots \tau^x \ldots \tau^l\right]_{i,y}$ |
| $N_j$ | $\left[s^1 s^2 \ldots s^x \ldots s^l \,\|\| \tau^1 \tau^2 \ldots \tau^x \ldots \tau^l\right]_{j,i}$ | $\left[11\ldots1\ldots1 \| 11\ldots1\ldots1\right]_{j,j}$ | ... | $\left[s^1 s^2 \ldots s^x \ldots s^l \,\|\| \tau^1 \tau^2 \ldots \tau^x \ldots \tau^l\right]_{j,y}$ |
| $N_k$ | $\left[s^1 s^2 \ldots s^x \ldots s^l \,\|\| \tau^1 \tau^2 \ldots \tau^x \ldots \tau^l\right]_{k,i}$ | $\left[s^1 s^2 \ldots s^x \ldots s^l \,\|\| \tau^1 \tau^2 \ldots \tau^x \ldots \tau^l\right]_{k,j}$ | – | $\left[s^1 s^2 \ldots s^x \ldots s^l \,\|\| \tau^1 \tau^2 \ldots \tau^x \ldots \tau^l\right]_{k,y}$ |
| $N_l$ | $\left[s^1 s^2 \ldots s^x \ldots s^l \,\|\| \tau^1 \tau^2 \ldots \tau^x \ldots \tau^l\right]_{l,i}$ | $\left[s^1 s^2 \ldots s^x \ldots s^l \,\|\| \tau^1 \tau^2 \ldots \tau^x \ldots \tau^l\right]_{l,j}$ | ... | $\left[s^1 s^2 \ldots s^x \ldots s^l \,\|\| \tau^1 \tau^2 \ldots \tau^x \ldots \tau^l\right]_{l,y}$ |
| . . . | . . . | . . . | . . . | |
| $N_x$ | $\left[s^1 s^2 \ldots s^x \ldots s^l \,\|\| \tau^1 \tau^2 \ldots \tau^x \ldots \tau^l\right]_{x,i}$ | $\left[s^1 s^2 \ldots s^x \ldots s^l \,\|\| \tau^1 \tau^2 \ldots \tau^x \ldots \tau^l\right]_{x,j}$ | ... | $\left[s^1 s^2 \ldots s^x \ldots s^l \,\|\| \tau^1 \tau^2 \ldots \tau^x \ldots \tau^l\right]_{x,y}$ |
| $N_y$ | $\left[s^1 s^2 \ldots s^x \ldots s^l \,\|\| \tau^1 \tau^2 \ldots \tau^x \ldots \tau^l\right]_{y,i}$ | $\left[s^1 s^2 \ldots s^x \ldots s^l \,\|\| \tau^1 \tau^2 \ldots \tau^x \ldots \tau^l\right]_{y,j}$ | ... | $\left[11\ldots1\ldots1 \| 11\ldots1\ldots1\right]_{y,y}$ |

*where* $\left[s^1 s^2 \ldots s^x \ldots s^l \,\|\| \tau^1 \tau^2 \ldots \tau^x \ldots \tau^l\right]_{i,j} = \left[s_{i,j}^{1-st} s_{i,j}^{2-nd} \ldots s_{i,j}^{x-th} \ldots s_{i,j}^{l-th} \,\|\| \tau_{i,j}^{1-st} \tau_{i,j}^{2-nd} \ldots \tau_{i,j}^{x-th} \ldots \tau_{i,j}^{l-th}\right]$ *and*

$\tau^1 \tau^2 \ldots \tau^x \ldots \tau^l = 11\ldots1\ldots1$ *in initial trust phase, and* $n = 2l$ *(bits).*

The node or the immediate node calculates the trust evolution values by equation (4), individually.

$$\tau_{i,j} = f_T(s_{i,j}^{1st}, s_{i,j}^{2nd}, \ldots, s_{i,j}^{l-th}) \tag{4}$$

where $f_T(\bullet)$ is a type of evolution function, where Genetic Algorithms (GAs) will be deployed and described later in the following paragraphs.

**Step 2:** Once all nodes have gathered all reply packets, the neighbor evolution information table will be updated.

**Step 3:** Then, the TA node $N_{TA}$ will broadcast periodically the query message with updated trust values to all neighboring nodes, in order to collect the information for constructing the network topology while satisfying the distinct cooperative score and updated trust evolution values.

### 3.3 Evolution Function using the GA Approach

In this section, the evolution function using the GA approach will be proposed. Thus, the goal of the trusted route selection, the chromosome code, initial population, fitness function and genetic operations

are formulated in order to establish a cooperative trusted routing path. Finally, Example 1 is also proposed in this section.

### 3.3.1 The Goal of the Trusted Route Selection

Due to the trusted route selection works in the WANETs including some dynamic malicious nodes, the goal of routing protocol is that any node could seek movement way from the initial node to the target node via the cooperative trusted evaluation procedure. This approach must meet the following conditions: (1) Does not have any collision with any malicious node; (2) Should be shortest.

### 3.3.2 Chromosome Code

The route is composed of consecutive path segments which are joined with a starting node, intermediate nodes and a target node. Corresponding to a path is an individual chromosome in the population. The path of the individual chromosome is expressed with a broken line which is joined with an uncertain number of nodes.

### 3.3.3 Initial Population

The initial population is produced according to the stochastic way; the given maximum hop of the individual is $m-1$ in advance, individual hop $x \in \{1,2,...,m-1\}$. There are $\frac{1}{2}(m \times m-1)$ fiducially marks which are $(N_1 \leftrightarrow N_2),(N_1 \leftrightarrow N_3),...,(N_2 \leftrightarrow N_3),(N_2 \leftrightarrow N_4),...,(N_{m-1} \leftrightarrow N_m)$ produced stochastically according to the following steps: embark from the initial node which launches a transmission request, a node adjacent to the initial node is selected stochastically as the next hop in the signal coverage area, so repeatedly, until the target point is found.

### 3.3.4 Fitness Function

Fitness function measures a good degree of each individual in the community to close the optimal solution in the evolution computation. The route of superior and inferior degrees is evaluated by the fitness value of the chromosome in the genetic algorithm. Therefore, the Cooperative Trust Route Searching Procedure (CTRS Procedure, for short) will be proposed in Procedure 4 later for construction of the fitness function in order to meet the requirement of the cooperative trusted routing. The CTRS Procedure will be described later.

### 3.3.5 Genetic Operations

Genetic operations include selection operation, crossover operation and mutation operation. These three kinds of operations have been introduced in subsection 2.1 and their method choice to be adopted in our algorithm.

**Example 1:**

It is assumed that the TA node $N_{TA}$ broadcasts the hello packet for discovering the trust-based topology in the WANET. The format of the hello packet is shown in Fig. 7.

After receiving the hello packet from the TA node or the delivering packet from other neighboring nodes, each node will update her/his CNI table and reply with the judged reputation packet which consists of her/his neighboring reputation values back to the TA node. Then, the trust evaluation table will be collected and created by a TA node as shown in Table 3. For instance, it assumed that there are

| Type | Hello Packet |
|---|---|
| Node ID | $N_{TA}$ |
| Node IP address | 224.0.2.0~224.0.255.255 |
| Node Mac address | 00.00.00.00.00.00<br>~FF.FF.FF.FF.FF.FF |
| Sequence number | 00000001 |
| Life time | 100 (Mini Seconds) |

Figure 7: An example of the hello packet format.

eight nodes plus a TA node in which the corresponding reputation values are judged by each other's neighboring nodes deployed in the WANET. After collecting all reputation values judged by each node, the TA node will perform Procedure 3.

**Procedure 3:**

**Step 1:** Let $x = 1$ for initial cooperative condition;

**Step 2:** At first, the judged values of reputation under the cooperative condition $E_{i,j}^{x-th}$ are formulated as $T_{i,j}^{x-th_{(10)}}$ which are supposed and shown in Fig. 8.

$$T_{i,j}^{x-\mathrm{th}_{(10)}} = \begin{array}{c|cccccccc} \mathrm{J_j} \backslash \mathrm{E_i} & N_1 & N_2 & N_3 & N_4 & N_5 & N_6 & N_7 & N_8 \\ N_1 & 15 & 3 & 9 & 9 & 10 & 12 & 4 & 14 \\ N_2 & 1 & 15 & 2 & 1 & 2 & 2 & 1 & 2 \\ N_3 & 10 & 4 & 15 & 6 & 9 & 7 & 5 & 11 \\ N_4 & 14 & 1 & 10 & 15 & 14 & 12 & 3 & 15 \\ N_5 & 11 & 4 & 7 & 10 & 15 & 10 & 4 & 14 \\ N_6 & 9 & 5 & 11 & 8 & 5 & 15 & 6 & 10 \\ N_7 & 7 & 7 & 11 & 7 & 10 & 9 & 15 & 12 \\ N_8 & 11 & 6 & 6 & 14 & 15 & 6 & 2 & 15 \end{array}$$

Figure 8: The $T_{i,j}^{x-th_{(10)}}$.

**Step 3:** Each column will be the computed average of the trust evaluation which is represented as the reputation for each node. The average function of the trust evaluation is shown as equation (5).

$$f_{i,ave} = \frac{1}{m} \sum_{j=1, j\neq i}^{m} t_{i,j} \times w \tag{5}$$

where $0 < w \leq 1$ is the weight value decided by the system.

**Step 4:** Each decimal-based element in $T_{i,j}^{x-th_{(10)}}$ will be transferred to the binary-based element and into $T_{i,j}^{x-th_{(2)}}$. Thus, the $T_{i,j}^{x-th_{(2)}}$ is listed in Fig.9.

$T_{i,j}^{x-\mathrm{th}_{(2)}} =$

| $J_j \backslash E_i$ | $N_1$ | $N_2$ | $N_3$ | $N_4$ | $N_5$ | $N_6$ | $N_7$ | $N_8$ |
|---|---|---|---|---|---|---|---|---|
| $N_1$ | 1111 | 0011 | 1001 | 1001 | 1010 | 1100 | 0100 | 1110 |
| $N_2$ | 0001 | 1111 | 0010 | 0001 | 0010 | 0010 | 0001 | 0010 |
| $N_3$ | 1010 | 0100 | 1111 | 0110 | 1001 | 0111 | 0101 | 1011 |
| $N_4$ | 1110 | 0001 | 1010 | 1111 | 1110 | 1100 | 0011 | 1111 |
| $N_5$ | 1011 | 0100 | 0111 | 1010 | 1111 | 1010 | 0100 | 1110 |
| $N_6$ | 1001 | 0101 | 1011 | 1000 | 0101 | 1111 | 0110 | 1010 |
| $N_7$ | 0111 | 0111 | 1101 | 0111 | 1010 | 1001 | 1111 | 1100 |
| $N_8$ | 1101 | 0110 | 0110 | 1110 | 1111 | 0110 | 0010 | 1111 |

Figure 9: The $T_{i,j}^{x-th_{(2)}}$.

**Step 5:** Each column will be sorted by the equation (6) as below.

$$S_i = sort_{j=1, j\neq i}^{m}(t_{i,j}) = [t_{i,j}], j = 1,2,...,m, \forall i = 1,2,...,n. \tag{6}$$

**Step 6:** Each column $j$ will perform the genetic operations as shown in the three steps as below.

**Step 6-a:** Selection operation

After sorting the $T_{i,j}^{x-th_{(2)}}$, the top 6 nodes with each having an evaluated value larger than $f_{i,ave}$ in Fig. 10.a except the evaluated node herself/himself will be selected into three pairs in order to perform a crossover and mutation operation. For instance, the top 6 nodes consist of three pairs, $\{(N_4,N_8),(N_5,N_3),(N_6,N_7)\}$, are selected in column 1. Then, the details of the crossover and mutation operation are described as below:

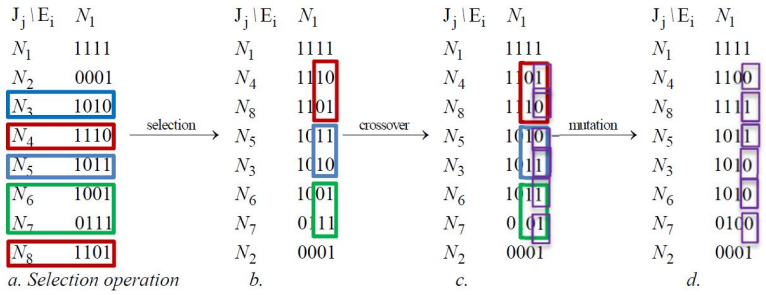


Figure 10: For columns 2 to 8, the steps are same as Step 6-a, Step 6-b and Step 6-a.

$$t_{i,j} = t_{4,1} = [1110] \text{ and } t_{i,j} = t_{8,1} = [1101] \xrightarrow{\text{crossover}} tc_{i,j} = tc_{4,1} = [1101] \text{ and } tc_{i,j} = tc_{8,1} = [1110]$$

$$t_{i,j} = t_{5,1} = [1011] \text{ and } t_{i,j} = t_{3,1} = [1010] \xrightarrow{\text{crossover}} tc_{i,j} = tc_{5,1} = [1010] \text{ and } tc_{i,j} = tc_{3,1} = [1011]$$

$$t_{i,j} = t_{6,1} = [1001] \text{ and } t_{i,j} = t_{7,1} = [0111] \xrightarrow{\text{crossover}} tc_{i,j} = tc_{6,1} = [1011] \text{ and } tc_{i,j} = tc_{7,1} = [0101]$$

Figure 11: Crossover operation.

**Step 6-b:** Crossover operation (shown in Fig. 11)

The details of the crossover operation as shown in Fig. 10.a, Fig. 10.b, and Fig. 10.c.

**Step 6-c:** Mutation operation (shown in Fig. 12)

$$tc_{i,j} = tc_{4,1} = [1101] \text{ and } tc_{i,j} = tc_{8,1} = [1110] \xrightarrow{\text{mutation}} tm_{i,j} = tm_{4,1} = [1110] \text{ and } tm_{i,j} = tm_{8,1} = [1111]$$

$$tc_{i,j} = tc_{5,1} = [1010] \text{ and } tc_{i,j} = tc_{3,1} = [1011] \xrightarrow{\text{mutation}} tm_{i,j} = tm_{5,1} = [1011] \text{and } tm_{i,j} = tm_{3,1} = [1010]$$

$$tc_{i,j} = tc_{6,1} = [1011] \text{ and } tc_{i,j} = tc_{7,1} = [0101] \xrightarrow{\text{mutation}} tm_{i,j} = tm_{6,1} = [1010] \text{and } tm_{i,j} = tm_{7,1} = [0100]$$

Figure 12: Mutation operation.

**Step 7:** Finally, the cooperative trust evaluations will be obtained by the TA node as shown in Fig. 5. The $TM_{i,j}^{x-th_2}$ is shown in Fig. 13.

$$\mathrm{TM}_{i,j}^{x-\mathrm{th}_{(2)}} = \begin{bmatrix} \mathrm{J_j \backslash E_i} & N_1 & N_2 & N_3 & N_4 & N_5 & N_6 & N_7 & N_8 \\ N_1 & 1111 & 0001 & 1011 & 1001 & 1011 & 1101 & 0101 & 1110 \\ N_2 & 0001 & 1111 & 0010 & 0001 & 0010 & 0010 & 0001 & 0010 \\ N_3 & 1010 & 0100 & 1111 & 0110 & 1000 & 0111 & 0111 & 1011 \\ N_4 & 1100 & 0001 & 1000 & 1111 & 1110 & 1101 & 0011 & 1101 \\ N_5 & 1011 & 0110 & 0111 & 1011 & 1111 & 1000 & 0101 & 1111 \\ N_6 & 1010 & 0101 & 1000 & 1000 & 0100 & 1111 & 0100 & 1010 \\ N_7 & 0100 & 0111 & 1110 & 0111 & 1011 & 1011 & 1111 & 1110 \\ N_8 & 1111 & 0110 & 0110 & 1111 & 1111 & 0110 & 0010 & 1111 \end{bmatrix}$$

$$= \begin{bmatrix} \mathrm{J_j \backslash E_i} & N_1 & N_2 & N_3 & N_4 & N_5 & N_6 & N_7 & N_8 \\ N_1 & \tau_{1,1}^{x-th} & \tau_{1,2}^{x-th} & \tau_{1,3}^{x-th} & \tau_{1,4}^{x-th} & \tau_{1,5}^{x-th} & \tau_{1,6}^{x-th} & \tau_{1,7}^{x-th} & \tau_{1,8}^{x-th} \\ N_2 & \tau_{2,1}^{x-th} & \tau_{2,2}^{x-th} & \tau_{2,3}^{x-th} & \tau_{2,4}^{x-th} & \tau_{2,5}^{x-th} & \tau_{2,6}^{x-th} & \tau_{2,7}^{x-th} & \tau_{2,8}^{x-th} \\ N_3 & \tau_{3,1}^{x-th} & \tau_{3,2}^{x-th} & \tau_{3,3}^{x-th} & \tau_{3,4}^{x-th} & \tau_{3,5}^{x-th} & \tau_{3,6}^{x-th} & \tau_{3,7}^{x-th} & \tau_{3,8}^{x-th} \\ N_4 & \tau_{4,1}^{x-th} & \tau_{4,2}^{x-th} & \tau_{4,3}^{x-th} & \tau_{4,4}^{x-th} & \tau_{4,5}^{x-th} & \tau_{4,6}^{x-th} & \tau_{4,7}^{x-th} & \tau_{4,8}^{x-th} \\ N_5 & \tau_{5,1}^{x-th} & \tau_{5,2}^{x-th} & \tau_{5,3}^{x-th} & \tau_{5,4}^{x-th} & \tau_{5,5}^{x-th} & \tau_{5,6}^{x-th} & \tau_{5,7}^{x-th} & \tau_{5,8}^{x-th} \\ N_6 & \tau_{6,1}^{x-th} & \tau_{6,2}^{x-th} & \tau_{6,3}^{x-th} & \tau_{6,4}^{x-th} & \tau_{6,5}^{x-th} & \tau_{6,6}^{x-th} & \tau_{6,7}^{x-th} & \tau_{6,8}^{x-th} \\ N_7 & \tau_{7,1}^{x-th} & \tau_{7,2}^{x-th} & \tau_{7,3}^{x-th} & \tau_{7,4}^{x-th} & \tau_{7,5}^{x-th} & \tau_{7,6}^{x-th} & \tau_{7,7}^{x-th} & \tau_{7,8}^{x-th} \\ N_8 & \tau_{8,1}^{x-th} & \tau_{8,2}^{x-th} & \tau_{8,3}^{x-th} & \tau_{8,4}^{x-th} & \tau_{8,5}^{x-th} & \tau_{8,6}^{x-th} & \tau_{8,7}^{x-th} & \tau_{8,8}^{x-th} \end{bmatrix}$$

Figure 13: The $TM_{i,j}^{x-th_2}$.

**Step 8:** If $x < 1$ then $x = x + 1$ and go to Step 2;

**Step 9:** After collecting and performing steps 2 through 8, the judged values of the reputation under all possible cooperative conditions $E_{i,j}^{x-th}, \forall x = 1,2,...,l$ will be updated into Table 2 as Table 3 for providing the updated $n$-TCBRT table.

**Step 10:** Ca will broadcast the $n$-TCBRT table to each node in the WANET.

**Procedure 4:** CTRS Procedure

When a node wants to deliver data to another node, the source node will compute a route to the destination node by using the CTRS Procedure, for short and referring the latest $n$-TCBRT. Next, it could quickly establish the connection via this route. The $n$-TCBRT represents a graph which shows the network topology. The CTRS Procedure for the route searching process is illustrated below. It is able to find the best neighbors for the route according to CTRS Procedure and updating the $n$-TCBRT, which has the highest cooperative trust evaluation with the lowest route cost.

The detail CTRS Procedure is shown in Fig 14 and Fig 15.

# 4 Discussions and Security Analyses

In this section, we analyze the security of the CTRS Procedure with respect to our main design goal for preventing and also reducing the damages from the InTs in the WANETs.

## 4.1 Filtering compromised node and selfish or non-honest node

It is assumed that if a relay node $N_k$, in a determined route in which two nodes $N_i$ and $N_j$ want to deliver the packet data to each other, is compromised or damaged by insider threats in this WANET communication system, then its neighboring nodes will also examine themselves to determne whether a compromised node or a selfish node may have altered its behavior in practice. For instance, upon checking many packet data or query messages sent to the other nodes, there are always no deliveries or no response, which often leads to losing the packet data or query fail. Specifically, the cooperative trust evaluation could provide protection by the high-score route in the CTRS Procedure for the delivery process in order to prevent InTs.

The CTRS Procedure proposed in this paper is a special type of behavioral-based technique that incorporates the designed cooperative trust evaluation to cope with compromised nodes and selfish nodes. Precisely speaking, all the packet data will be routed within only trusted nodes having the high scores of cooperation evaluations which are periodically measured and then updated by all the cooperative nodes. It has the ability to locate and filter the compromised node and selfish or non-honest node mentioned above.

Moreover, upon receiving the periodically broadcasted the query message with updated trust evaluation values by other node, each node will also update her/his CNI table. Finally, the $n$-TCBRT maintained by each node will be immediately updated and synchronized as referred to in the CNI table.

In the other words, if a source node $N_i$ sends a packet data to the destination node $N_j$, the packet data will be delivered according to the CTR set outputted by Procedure 4. Then, the source node $N_i$ is able to send a packet data to the destination node $N_j$ along with the CTR set including a primary route together with some candidate routes. If any relay node finds something wrong in the routing process, it means that there are some insider threats in the routing environment. Therefore, the relay node will update the CNI table and report to the TA node in order to update the $n$-TCBRT. Finally, the new route table will be kept on the highest cooperative evaluations with lowest route cost again. Therefore, the

| | |
|---|---|
| *Input:* | *Source node $N_i$ ; Destination node $N_j$ ; n-TCBRT;* |
| *Output:* | *A set of cooperative trust route (CTR set, for short );* |
| *Begin* | |
| *Step 1*: | *Let the nodes $N_i$ and $N_j$ for the x-th cooperative evaluations, and the initial value be the matrix as following* $\left[s^1 s^2 ... s^x ... s^l \,||\, \tau^1 \tau^2 ... \tau^x ... \tau^l\right] = \left[11...1...1 \,||\, 11...1...1\right]$ ; |
| *Step 2*: | *Let $w = 1$ ; let $N_r \leftarrow N_i$ and let $N_k \leftarrow N_j$ for initial value, where $N_r$ and $N_k$ are assumed as the variables of the relay node, and the notation " $A \leftarrow B$ " means that the content of variable B is stored into the variable A ;* |
| *Step 3*: | *Select the unchecked nodes $N_r$ , and perform the "AND" bitwise operation denoted as " $\bullet$ " with the nodes $N_k$ to find satisfactory cooperative evaluations on the n-TCBRT. Such that* $\left[s_{r,k}{}^{x\text{-}th}, \forall x \in \{1,2,...x,...l\}\right] \bullet \left[\tau_{r,k}{}^{x\text{-}th}, \forall x \in \{1,2,...x,...l\}\right]$ *equals to* $\left[s^1 \bullet \tau^1 \,||\, s^2 \bullet \tau^2 \,||\, ... \,||\, s^x \bullet \tau^x \,||\, ... \,||\, s^l \bullet \tau^l\right]$ ; |
| *Step 4*: | *Check the neighboring node to find the connectable route approved for the x-th cooperative evaluations;*<br>*4a. If* $\left(s_{r,k}{}^{x\text{-}th} \bullet \tau_{r,k}{}^{x\text{-}th}\right) = 1$ *, then there is a route approved for the x-th cooperative evaluations between the node $N_r$ and $N_k$ ; In addition,*<br>*if the node $N_k = N_j$ then the connectable route $N_r \leftrightarrow N_k \Rightarrow N_i \leftrightarrow N_j$ is found, where the notation " $N_x \leftrightarrow N_y$ " means that the node $N_x$ has a connectable route to the node $N_y$ ; then add the route $N_r \leftrightarrow N_k$ to the set of cooperative route vectors; and then proceed to Step 6 ;*<br>*unless if it only finds the middle connectable route $N_r \leftrightarrow N_k$ ; then add the route $N_r \leftrightarrow N_k$ to the set of cooperative route vectors; furthermore, select the next neighboring node $N_w, w \in \left\{1,2,...,\left|N^{x-th}\right|\right\}$ satisfied the same x-th cooperative evaluations; additionally,*<br>*if $w \le \left|N^{x-th}\right|$ , let $N_k \leftarrow N_w$ ; and then proceed to Step 3;*<br>*then go to Step 4b;*<br>*end if;*<br>*end if;*<br>*Else if*<br>$\left(s_{r,k}{}^{x\text{-}th} \bullet \tau_{r,k}{}^{x\text{-}th}\right) = 0$ *then there is no route approved for the x-th cooperative evaluations between the node $N_i$ to the node $N_k$ ; Select the next neighboring node $N_w, w \in \left\{1,2,...,\left|N^{x-th}\right|\right\}$ satisfied the same x-th cooperative evaluations;*<br>*if $w \le \left|N^{x-th}\right|$ , let $N_k \leftarrow N_w$ ; and then proceed to Step 3;*<br>*else if*<br>*then proceed to Step 4b;*<br>*end if;*<br>*End if;*<br>*4b. let $N_x \leftarrow N_k$ which acts as the immediate border node which satisfies the same x-th cooperative evaluations; and let the value $x' \leftarrow x+1$ for the next external (x+1)-th cooperative evaluations; and find the $N_y$ which has the connectable route $N_x \leftrightarrow N_y$ to the immediate border node. It then satisfies the next external (x+1)-th cooperative evaluations; also add the route $N_x \leftrightarrow N_y$ to the set of cooperative route vectors;* |

Figure 14: The CTRS Procedure (1).

| | |
|---|---|
| Step 5: | *Check the neighboring nodes of $N_y$ to find the connectable route as it satisfies the next external $x'$-th cooperative evaluations;*<br>*5a. Select an unchecked node $N_z$ which is the neighboring node of $N_y$, and perform the "AND" operation with the node $N_y$ depending on the n-TCBRT. Thus, the $x'$-th cooperative evaluations of unchecked neighboring nodes between the nodes $N_y$ and $N_z$ is as $\left(s_{y,z}^{x'\text{-th}} \bullet \tau_{y,z}^{x'\text{-th}}\right)$ ;*<br>*If $\left(s_{y,z}^{x'\text{-th}} \bullet \tau_{y,z}^{x'\text{-th}}\right)=1$ ; add the route $N_y \leftrightarrow N_z$ to the set of cooperative route vectors; and*<br>*if the node $N_z = N_j$ , then proceed to Step 6 ;*<br>*if it only find the middle connectable route $N_y \leftrightarrow N_z$ ; then add the route $N_y \leftrightarrow N_z$ to the set of cooperative route vector; furthermore, select the next neighboring node $N_w, w \in \left\{1,2,...,\left\|N^{x'-th}\right\|\right\}$ satisfied the same $x'$-th cooperative evaluations; moreover; additionally,*<br>*if $w \leq \left\|N^{x'-th}\right\|$, let $N_z \leftarrow N_w$ ; and then proceed to Step 5a;*<br>*then go to Step 5b;*<br>*end if;*<br>*end if;*<br>*End If*<br>*Else if*<br>*$\left(s_{y,z}^{x'\text{-th}} \bullet \tau_{y,z}^{x'\text{-th}}\right)=0$ then there is no route approved for the $x'$-th cooperative evaluations between the node $N_y$ to the node $N_z$ ; Select the next neighboring node $N_w, w \in \left\{1,2,...,\left\|N^{x'-th}\right\|\right\}$ satisfied the same $x'$-th cooperative evaluations;*<br>*if $w \leq \left\|N^{x'-th}\right\|$, let $N_z \leftarrow N_w$ ; and then proceed to Step 5a;*<br>*else if*<br>*then proceed to Step 5b;*<br>*end if;*<br>*End if;*<br>*5b. let $N_{x+1} \leftarrow N_z$ which acts as the immediate border node and satisfies the same $x'$-th cooperative evaluations. Let the value $x'' \leftarrow x'+1$ represent the next external $(x+2)$-th cooperative evaluations; and find the $N_{y+1}$ which has the connectable route $N_{x+1} \leftrightarrow N_{y+1}$ this is then the immediate border node which satisfies the next external $(x+2)$-th cooperative evaluations; also add the route $N_{x+1} \leftrightarrow N_{y+1}$ to the set of cooperative route vectors;* |
| Step 6: | *Similarly, the cooperative evaluations route searching works in a similar way until the route vector $\left[N_i \leftrightarrow N_j\right]=\left[\left(N_i \leftrightarrow N_{i+1}\right)\|\|\left(N_{i+1} \leftrightarrow N_{i+2}\right)\|\|...\|\|\left(N_{j-1} \leftrightarrow N_j\right)\right]$ is found, when all possible neighboring nodes are checked for all of $x$-th cooperative evaluations, recursively;* |
| Step 7: | *Output the set of CTRV including a primary route together with some candidate routes;* |
| *End;* | |

Figure 15: The CTRS Procedure (2).

CTRS Procedure proposed in this paper could filter the compromised node and selfish or non-honest node in order to prevent the unexpected routing interruption and injected false route among any two communication nodes in routing process.

### 4.2 Reduction of the damage from InTs in the WANETs

After periodically updating a new routing $n$-TCBRT table, the routing paths will be updated in order to reduce the damages from InTs in the WANETs. It is assumed that there is a compromised node t $N_k$ that wants to compromise the routing task. Procedure 4 is proposed to generate a CTR set using the $n$-TCBRT. Each node will broadcast periodically the query message with updated trust evaluation values to the TA node in order to ensure that the relay nodes truly forward the packet data sent from the source node, and also judge whether its neighbors are normal or have a compromised node, selfish node or unselfish node. Upon receiving the periodically broadcasted query message with the updated trust evaluation values by other nodes, each received node will also update its CNI table. Finally, the $n$-TCBRT maintained by the TA node will be immediately updated and synchronized as referred to in the CNI table. Therefore, each node will then check whether if many packet data or query messages sent to the neighboring node will often leads to losing the packet data or having a failed query. To proactively prevent the various malicious attacks, the TA node will periodically renew the $n$-TCBRT. Thus, this approach will prevent some compromised nodes from inflicting further damage and will the damage from InTs in the WANETs.

### 4.3 Comparison with the TCBRP scheme

There are four items between the CTBRP and the TCBRP scheme [5] described in this subsection. The compared results are shown in Table 4.

Table 4: The comparisons between the CTBRP and the TCBRP scheme.

| Schemes / Compared Items | TCBRP scheme | CTBRP |
|---|---|---|
| Which optimal algorithm is adopted? | none | GA algorithm |
| Is there any cooperative route selection algorithm? | Yes | Yes |
| Is there any cooperative trust evaluation? | Yes | Yes |
| Could it deal with the route fault tolerance? | Yes | Yes |

## 5 Conclusions

We have considered that the majority of insider threats come from untrusted users who are fully authorized to use the WANET systems they are accessing. The CTBRP using the $n$-CTBRT is proposed in this paper for ensuring the trusted routing table in order to reduce the damages from InTs in the WANETs. Specifically, the cooperation trust evaluation using the GA is employed in this paper for evaluating the inside nodes which are fully authorized to communicate in the WANET. According to the CTBRP, the source node could send the packet data to the destination node along with the CTR set of cooperative trust

evaluations route vector including a primary route together with some candidate routes. This approach is a type of behavioral-based evaluation technique. For example, the compromised node and the selfish or non-honest node will be evaluated by its neighboring nodes. Once a relay node has been compromised or damaged by insider threats in the WANET, it will attempt to damage any two nodes' routing. Therefore, the proposed CTBRP in this paper not only evaluates the behavior of the compromised node or a selfish node, but also efficiently reduces the damages from InTs in the WANETs.

### Acknowledgements

This work was supported in part by the Ministry of Science and Technology, Taiwan, Republic of China, under Grant MOST 103-2221-E-468-027, also by Asia University, Taiwan, under Grant 101-asia-28.

## References

[1] W. Bai, B. Xue, and Y. Sun. Research on path planning for soccer robot based on improved genenic algorithm. In *Proc. of the International Conference on Mechatronic Science, Electric Engineering and Computer (MEC'11), Jilin, China*, pages 1687–1690. IEEE, August 2011.

[2] H.-C. Chen, T. Chen, H. Fang, and Z. Sun. A routing algorithm based on event-oriented applications for digital home wireless heterogeneous networks. *International Journal of Engineering and Industries*, 2(3):96–103, September 2011.

[3] H.-C. Chen, N.-Y. Shih, R. Noviyanto, and J.-C. Chen. A cooperative bit-map routing protocol in ad hoc networks. In *Proc. of the 7th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS'13), Taichung, Taiwan*, pages 325–330. IEEE, July 2013.

[4] H.-C. Chen and K. Wattanachote. A role-oriented routing algorithm applied for wireless heterogeneous networks. In *Proc. of the 5th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS'11), Seoul, Korea*, pages 420–423. IEEE, June 2011.

[5] H.-C. C. J. Chen) and J.-Y. Lin. A trust-based cooperation bit-map routing protocol for ad hoc networks. In *Proc. of the 8th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA'13), Compiegne, France*, pages 539–544. IEEE, October 2013.

[6] Y.-S. Chen, C.-H. Cho, I. You, and H.-C. Chao. Cross-layer design for improved qoe in content distribution networks. *Simulation Modelling Practice and Theory*, 19(8):1723–1744, September 2011.

[7] M. Elkotob and K. Andersson. Cross-layer design for improved qoe in content distribution networks. *IT CoNvergence PRActice (INPRA)*, 1(1):37–52, March 2013.

[8] H. Kim, S. Lee, and C. Kim. Design of knowledge discovery agent for a bit-map on ad hoc mobile networks. In *Proc. of the 1st KES Symposium on Agent and Multi-Agent Systems – Technologies and Applications, Wroclaw, Poland, LNCS*, volume 4496, pages 738–746. Springer-Verlag, May-June 2007.

[9] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin. Grs: The green, reliability, and security of emerging machine to machine communications. *IEEE Communications Magazine*, 49(4):28–35, April 2011.

[10] R. Lu, X. Lin, H. Zhu, X. Liang, and X. Shen. Becan: A bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 23(1):32–43, January 2012.

[11] MissionMode. Effective incident management: Insider security threats. `http://www.missionmode.com/blog/insider-threats-are-a-serious-cyber-security-issue/`, April 9, 2013.

[12] A. Oberle, A. Rein, J. Paatero, A. Lunn, and P. Racz. Integrating trust establishment into routing protocols of today's manets. In *Proc. of the 2013 IEEE Wireless Communications and Networking Conference (WCNC'13), Shanghai, China*, pages 2369–2374. IEEE, April 2013.

[13] A. Zaritsky. Introduction to genetic algorithms. `www.cs.bgu.ac.il/~sipper/courses/ecal051/assaf-ga.ppt`.

[14] X. Zhang, X. Gao, D. Shi, and D. K. Sung. Lifetime-aware leisure degree adaptive routing protocol for mobile ad hoc networks. In *Proc. of the 3rd Internatiional Conference on Wireless and Mobile Communications (ICWMC'07), Guadeloupe, French*, pages 1–6. IEEE, March 2007.

[15] L. Zhao, A. Y. Al-Dubai, and G. Min. Cross layer neighbourhood load routing for wireless mesh networks. In *Proc. of the 24th IEEE International Parallel and Distributed Processing Symposium (IPDPS'10), Atlanta, USA*, pages 1–7. IEEE, April 2010.

[16] F. Zou, X. Zhang, X. Gao, D. Shi, and E. Wang. Load balance routing using packet success rate for mobile ad hoc networks. In *Proc. of the 2007 International Conference on Wireless Communications, Networking and Mobile Computing (WICOM'07), Shanghai, China*, pages 1624–1627. IEEE, September 2007.

---

## Author Biography

**Hsing-Chung Chen (Jack Chen)** received the B.S. degree in Electronic Engineering from National Taiwan University of Science and Technology, Taiwan, in 1994, and the M.S. degree in Industrial Education from National Normal University, Taiwan, in 1996, respectively. He received the Ph.D. degree in Electronic Engineering from National Chung Cheng University, Taiwan, in 2007. During the years 1991-2007, he had served as a Mobile Communication System Engineer at the Department of Mobile Business Group, Chunghwa Telecom Co., Ltd. From Feb. 2008 to Feb. 2013, he was the Assistant Professor of the Department of Computer Science and Information Engineering at Asia University, Taiwan. Since February 2013–present, he is the Associate Professor of the Department of Computer Science and Information Engineering at Asia University, Taiwan. Currently, he is interested in Information Security, Cryptography, Role-based Access Control, Computer Networks and Heterogeneous networks. He was Program Co-Chair of EMC-2012, CISIS-2013, IMIS-2013. He is a member of CCISA, ICCIT, IET and IEEE. Dr. Chen was also the Editor-in-Chief of Newsletter of TWCERT/CC from July 2012 to June 2013.

**Hui-Kai Su** received the B.S degree from I-Shou University, Taiwan, in 1999. He received the M.S. degree and the Ph.D. degree from National Chung-Cheng University, in 2001 and 2006 respectively. He was an Assistant Professor at the department of computer science and information engineering, Nanhua University, Taiwan, during 2006 and 2009. He joined the department of electrical engineering, Formosa University, in the spring of 2009. Currently he is an Associate Professor in the department. His research interests include multimedia network applications, P2P network applications, IP/MPLS network survivability, network QoS control and management, embedded systems, etc.