SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

January 2014, Vol. 57 012111:1–012111:13
doi: 10.1007/s11432-012-4659-7

A secure routing model based on distance vector routing algorithm

WANG Bin[1,5*], WU ChunMing[1], YANG Qiang [2], LAI Pan[3],
LAN JuLong[4] & GUO YunFei[4]

[1]*College of Computer Science, Zhejiang University, Hangzhou* 310027*, China;*
[2]*College of Electrical Engineer, Zhejiang University, Hangzhou* 310027*, China;*
[3]*School of Computer Engineering, Nanyang Technological University, Singapore* 639798*, Singapore;*
[4]*National Digital Switching System Engineering and Technological Research Center, Zhengzhou* 450002*, China;*
[5]*Hangzhou Sunyard Technology Company Limited, Hangzhou* 310053*, China*

Received June 6, 2012; accepted September 3, 2012; published online October 31, 2012

Abstract Distance vector routing protocols have been widely adopted as an efficient routing mechanism in current Internet, and many wireless networks. However, as is well-known, the existing distance vector routing protocols are insecure as it lacks of effective authorization mechanisms and routing updates aggregated from other routers. As a result, the network routing-based attacks become a critical issue which could lead to a more deteriorate performance than other general network attacks. To efficiently address this issue, this paper, through analyzing the routing model and its security aspect, and presents a novel approach on guaranteeing the routing security. Based on the model, we present the security mechanism including the message exchange and update message security authentication mechanism. The suggested approach shows that the security mechanism can effectively verify the integrity and validate the freshness of routing update messages received from neighbor nodes. In comparison with exiting mechanisms (SDV, S-RIP etc), the proposed model provides enhanced security without introducing significant network overheads and complexity.

Keywords routing security, distance vector, auxiliary trustable model, authentication metric

Citation Wang B, Wu C M, Yang Q, et al. A secure routing model based on distance vector routing algorithm. Sci China Inf Sci, 2014, 57: 012111(13), doi: 10.1007/s11432-012-4659-7

1 Introduction

Information security has been a critical and challenging issue along with the development of current Internet infrastructure. Network routing protocol is one of the key aspects of the communication network which disseminations network topology information among routers, to enable optimal selection of end-to-end routing paths and forward data packets across the network. Without correct routing information, the packet transportation cannot be efficient carried out, and even worse, the network may collapse [1–3]. At present the design of routing protocols mainly focuses on the functions and performance, e.g. finding the shortest path, loop-free guarantee and convergence acceleration [4,5]. The implementation of these functions is firmly based on the assumption that the network nodes are trustworthy and the received

*Corresponding author (email: wbin2006@gmail.com)

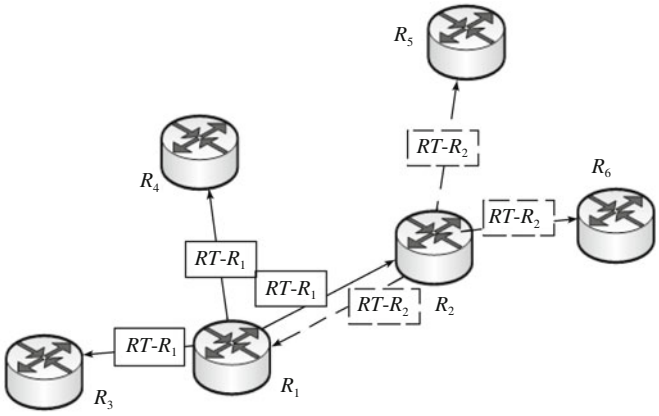

Figure 1 Routing information dissemination in distance vector routing protocols.

routing information is correct. However, such assumption can become invalid in realistic networks as the routing infrastructure is not reliable due to numerous reasons [6–8] and the two key reasons are as follows: 1) the existing routing protocols take none or little security mechanisms into consideration in its design so that the attackers can degrade the routing infrastructure by fabricating updating routing information; and 2) routing protocols generally do not have strategies to prevent the network from active attacks. As a result, the adversary users can inform other routers with false routing information, and hence attack the network.

Based on this motivation, this paper attempts to address the issue to promote and enhance the routing security of distance-vector routing protocols. Through analyzing the routing model and typical routing attacks, a novel secure and trustworthy routing model as well as the associated mechanism are presented.

2 Routing model based on distance vector routing algorithm

It is well known that the distance vector routing protocols are designed based on the Bellman-Ford algorithm [9], as routers forward dissemination their routing tables to their neighbor routers periodically. Upon receiving the routing tables, each router will compare the received information with its routing table, and update the routing table information accordingly. Afterwards, the router will continue to propagate its update routing table to other neighbor routers in the same manner.

With the distance vector routing protocols, the routing information maintained at the router is only made available to its neighbors and the routing information traverses one hot in the network. Figure 1 illustrated the routing information transmission scenario in distance vector routing protocols, with (RT-R_1) and (RT-R_2) representing the current routing tables of R_1 and R_2 respectively. It is shown in Figure 1 that R_1 and R_2 send their routing tables (RT-R_1) and (RT-R_2) to their neighbors and the neighbors do not forward the information to the routers located in the next-hop.

Base on the above description, we can summarize the features as follows: 1) for the network routers, the routing information only can be obtained from its neighbors; and 2) in the networks adopting distance vector routing protocols, the distance difference in terms of hops between the source node to destination node and the neighbor node to the destination node cannot be more than 1.

3 The routing security of distance vector routing protocols

In general, the routing security includes node security and communication security. The former refers to the access control of operating system and the access control privacy in the router; the latter mainly focuses on the security aspect of transporting and processing data. If there is no specially mentioned, the communication security and routing security are interchangeable throughout this paper.

3.1 Network routing protocol attacks

In this work, we restrict our view to the routing protocol attacks, which can be classified as active attacks and passive attacks [10,11]. The former tends to interrupt the operation, while the latter attempts to learn or use the information of the network during the attacks. However, the operation of passive attackers does not influence the network.

More specifically, the following attacks are related to the distance vector routing protocols:

1) Sniffing attack (passive): including inner attacks, and outer attacks. The attackers can monitor and record the transmission situation of data on a link or node and figure out the network situation for the purpose of attacks.

2) Forgery attack (active): references for each type of attacks: replacement attack, inserting attack, and impersonation attack.

3) Interruption attack (active): it aims at making legal routers unable to operate normally by interruption. This kind of attacks can be classified as follows: interference attack, overload attack.

4) Replay attack (active): the attacker sends obsolete routing information to legal routers.

3.2 Analysis of attacks

At present one of the most serious attack towards this kind of routing protocols is forgery attack that the attacker provides false updating routing information and these attacks. It can be further classified as follows:

1) Short-distance false routing information: the attacker declares that the distance from itself to a certain destination node is smaller than the real distance, or it declares that it is disconnected to the network to carry out attacks, e.g. black hole attack and hijack attack.

2) Long-distance false routing information: the attacker declares that the distance from itself to a certain destination node is larger than the real distance, so as to reduce the traffic transmission. As a result, the network resources are not properly utilized and network performance is degraded.

In fact, the attack of short-distance false routing information is more severe than the attack of long-distance false routing information. Given that a vicious node conducts attacks towards other nodes and it sends a false updating routing message (D, V_x, C), where the D is the destination of the route ID, V_x is the neighbor to the destination's next hop, C is the cost to the destination nodes. The influence range is analyzed as follows: It is assumed that the distance from a node N to the destination node D is D_2 while the distance from the attack node to node N is D_1. If A intends to deceive N successfully, C is required to satisfy the condition: $D_1 + C < D_2$, which is $C < D_2 - D_1$, and $C > 0$. Therefore, if the destination node satisfies the requirement, the false routing message sent from A to the destination node can deceive node N successfully.

In summary, the attack node position can be obtained which effectively determines the attack capacity. In particular, the threat towards the node becomes more serious as the attacker is nearer to the victim node. In the distance vector routing protocols, the exchanged routing messages updates from the neighbor nodes and sent by the node can be obtained through distributed computing. Therefore, in order to enhance the routing security, network node must guarantee the credibility of the updating routing message received from its neighbor nodes.

3.3 Distance vector routing protocols

Currently, the existing research efforts are confronted with the difficulty that the updating routing messages are made available from the computation with a distributed nature. In order to address this issue, numerous proposals on enhancing the security mechanisms are available. Based on applied technologies, current solutions can be classified as follows:

1) Routing information verification. In order to solve the acknowledgement problem in updating routing message, Mittal et al. [12] proposes a method of using sensor nodes to perceive a validate the network topology. However, the method assumes that the sensor nodes are required to be aware of the current network topology. In fact, the routers using distance vector routing protocols are not aware of

the topology of the entire network. Therefore, this method violates the design goal of distance vector routing protocols. Also this methodology cannot prevent the network from incorrect updating routing information propagation.

2) Hash chain based method. Hu et al. [13] proposed a method based on hash chain and certification tree to verify the correctness of distance. In fact, it can merely detect the attacks of short-distance false routing information and hence cannot defend the forgery attack.

3) S-RIP based method [14]. This mechanism uses MAC function with key to verify of routing information. The security mechanism is based on the symmetrical cryptosystem and it requires that each pair of nodes to establish the shared key. Therefore, the distribution and management of the key becomes the security bottleneck of the whole network. In addition, when using this method in the verifying the correctness of routing information, it is required to send request to nodes along the path and then the nodes will return a reply. This method will increase the network load greatly and cause new potential safety hazard.

4) The SDV mechanism [15]. This mechanism will integrate the routing database of Mittal and S-RIP and it requires the support of public key infrastructure (PKI). It is required that the trust nodes are implemented in the network. This method does not indicate the approach to implement the trust node and the relationship between the implement of the trust node and the size of the network topology. Thus, it is difficult to carry out. In addition, the implement of the trust node will be the bottleneck of the whole mechanism. Particularly, if the trust node collapses, the routing protocol cannot operate normally.

It can be seen from the review of current solutions that, currently no secure and efficient mechanisms to guarantee the security of distance vector routing protocols. This paper attempts to address and present a novel solution to enhance the security.

4 The security model of distance vector routing protocol-auxiliary trustable model

Through the above analysis of distance vector routing protocol, and apart from the verification of the integrity, freshness and source of the message, the verification of the routing related message correctness is also required to be made. The key of such verification is to verify the correctness of the updating routing message. To the author's best knowledge, there is little work in addressing this issue for the distance vector routing protocols. In this section, we present a novel trust security model–auxiliary trustable model to verify received messages at routers in the distributed networks environment.

4.1 The concept of auxiliary trustable model

The routing message dissemination of the distance vector routing protocol is implemented through distributed computing. The routing message of the neighbor node originates from its directed adjacent node. In the network topology of Figure 1, if node R_3 intends to verify the correctness of the message regarding the subnet connected with R_6, it is required to verify the message sent by R_2. The verification process will not terminate before the verification of the message of R_6 is completed. If this method is applied, the network load and delay will grow significantly when the node is far from the destination node, which leads to additional threats to the network operation. Thus, such process need to be improved to promote the security.

The auxiliary trustable model is to use the message provided by the auxiliary trustable node to verify the correctness of the messages received from the neighbor nodes and the messages to the neighbor originates from the auxiliary trustable node. In the distance vector routing protocols, the auxiliary trustable node is the adjacent node of the neighbor node.

4.2 The auxiliary trustable model

The nodes in the auxiliary trustable model can be classified as follows: 1) measurement root(MT), which refers to the entity of the security measurement; 2) measurement node, refers to the component carrying

out the security measurement and function, and performing the security measurement to the measurement node; and 3) auxiliary trustable node(AN), refers to the node auxiliary the measurement node to conduct the security of measurement of the measurement root.

The classification of the above nodes are based on a certain security metric. In different security measurement of a node, the corresponding types become distinct. The node set participating in a security measurement is expressed as $E = \{MT, MN, AN\}$, and $AN = \{AN_1, AN_2, \ldots, AN_n\}$. The node in must satisfy the following constrain set $L = \{l_1, l_2\}$:

$l_1 : MN \in H_{MT}$ represents the set of the nodes which belongs to the neighbor node set H_{MT} of MT;

$l_2 : RN \in H_{MT}$ means that the auxiliary trustable nodes are the neighbors of the measurement root node.

Definition 1. For a set of security measurement nodes, $E = \{MT, MN, AN\}$, where L represents the restraints, the following notations can signify the security relationships of the nodes:

1) The Freshness of the message (Fresh) is expressed as $Fresh(e_1, M)$ which means that the entity e_1 can assess whether a message M is fresh. That is to say, if M is the updating routing message sent from the entity e_1, it can be decided that M is the latest updating information.

2) The integrity certification of the message (Auth), denoted as $Auth(e, M)$, can verify if the message M is tampered with in the transmission.

3) The source certification of the message (Source), denoted as $Source(e_1, e_2) \longrightarrow M$, means e_1 verify M is generated by e_2.

4) The acknowledgement of the message acceptance (Accept), denoted as $Accept(e, M)$, means that the entity e acknowledge the acceptance of the message M.

5) The message source (Comp), denoted as $Comp\langle M|M_1, \ldots, M_n\rangle$, indicate that the message M is obtained by $Comp\langle M|M_1, \ldots, M_n\rangle$.

6) The measurement of the message is expressed as $Measure(MN, M_{MT})|\langle AN\rangle$, which means that the measurement node MN completes the correctness verification of the message sent by the measurement root under the assistance of the auxiliary trustable node set AN.

7) The entity trust is denoted as $Trust(MN, MT)|\langle L\rangle$. It represents the trust node MT of MN under the restraint, which also means that the message sent by MT is truthful.

8) The message trust (MesTru) is denoted as $MesTru(MN, M)$, which means that MN believes that the message M is correct.

Definition 2. The connection of the node set is $E = \{MT, MN, AN\}$ and the message set is $M = \{M_1, M_2, \ldots, M_n\}$(the message M_i is generated by the node i). The security rules are defined as follows:

1) The rule of the message acknowledgment

$$\frac{Fresh(MN, M), Auth(MN, M), Source(MN, MT \longrightarrow MN), (MN, MT)|\langle l_1\rangle}{Accept(MN, M)}. \tag{1}$$

If the freshness, integrity, and the source verification of the message M are confirmed, the message is received.

2) The rule of the acknowledgement of the information source

$$\frac{Accept(MN, \langle M_{MT}, M_{AN_1}, \ldots, M_{AN_n}\rangle), Accept(MN, \langle M_{MT}, M_{AN_1}, \ldots, M_{AN_n}\rangle)|\langle L\rangle}{Comp\langle M_{MT}|M_{AN_1}, \ldots, M_{AN_n}\rangle}. \tag{2}$$

If the node MN acknowledges the acceptance of the message $\langle M_{MT}, M_{AN_1}, \ldots, M_{AN_n}\rangle$ and MT acknowledges the acceptance of the message $\langle M_{N_1}, \ldots, M_{N_n}\rangle$, the node MN believes that M_{MT} is the result computed by $\langle M_{N_1}, \ldots, M_{N_n}\rangle$.

3) The rule of the auxiliary trustable

$$\frac{Comp\langle M_{MT}, M_{AN_1}, \ldots, M_{AN_n}\rangle, Measure(MN, M_{MT})|\langle M_{AN_1}, \ldots, M_{AN_n}\rangle}{Trust(MN, MT)|\langle L\rangle}. \tag{3}$$

If MN acknowledges the message M_{MT} is the result computed by $\langle M_{AN_1}, \ldots, M_{AN_n}\rangle$ and passes the measurement of M_{MT} under the assistance of $M_{AN_1}, \ldots, M_{AN_n}$, MN trusts MT which means that $RN = \{AN_1, AN_2, \ldots, AN_n\}$ assists MN to conduct the trust evaluation of MT.

4) The rule of the trust extension

$$\frac{Trust(MT, AN_1)|\langle L_1\rangle, \ldots, Trust(MT, AN_n)|\langle L_n\rangle, Comp\langle M_{MT}|M_{AN_1}, \ldots, M_{AN_n}\rangle}{Trsut(MN, \langle AN_1, \ldots, AN_n\rangle)}. \tag{4}$$

If MT trusts $AN = \{AN_1, AN_2, \ldots, AN_n\}$, M_{MT} is the result computed by $\langle M_{N_1}, \ldots, M_{N_n}\rangle$ and the corresponding restraints are satisfied, MN trusts $AN = \{AN_1, AN_2, \ldots, AN_n\}$.

5) The rule of the message trust

$$\frac{Trsut(e_1, e_3), Accept(e_1, M)|e_3 \longrightarrow M}{MesTru(e_1, M)}. \tag{5}$$

If e_1 trusts e_3 and e_1 acknowledges the acceptance of the message M under the restraint L_1, e_1 believes that the message M is truthful.

In the case that the security rules are met, the freshness, integrity, the source verification and the message correctness of the received updating message can be guaranteed. Nevertheless, the corresponding security mechanism is required in the security rule. The following section presents the security mechanisms to implement the security rules in the propose security model, i.e the method for message correctness verification and the mechanism of the message security verification.

4.3 The method of the message correctness verification

The security rule (2) requires the measurement root node to verify the correctness of the updating message, which is presented as follows:

4.3.1 *Assumptions and definitions*

The method correctness verification is based on two prerequisites: 1) the network convergence has been completed; and 2) the source and integrity of the received updating routing messages can be verified.

The method of the message correctness verification is to verify the messages which have passed the above verifications. The verification method introduces the following definitions.

Definition 3. The routing information base (RIB). Every node has a RIB and maintains all the latest received routing information with the date structure of (dest_{id}, neighbor, nexthop, cost). In the structure, dest_{id} represents the address of the destination node; neighbor means that the update creates the neighbor of the item which is also the next hop of the route; nexthop stands for the next hop from the neighbor node to the destination node; cost is the distance from the neighbor node to the destination node.

Definition 4. False routing information means the routing information in which the distance to the destination node one hop larger or smaller than that from the neighbor node to the destination node.

The node performs the following method of the message correctness verification in the following situations: 1) the node detects that the data sent to the destination node is discarded substantially; 2) the node finds that the measurement from the neighbor node to the destination node is evidently different from the measurement sent before; and 3) the network conducts the detection of the updating routing message sent by the neighbor node every time interval. The time frequency is set by network administrator according to the security demand.

4.3.2 *The method of the message correctness verification*

In the network adopting the distance vector routing protocol, after the protocol convergence is completed, the following conclusions can be reached: the absolute value of the difference between the hops from every node to the destination node and the hops from the neighbor node to the destination node is not larger than 1. As is shown in Figure 2, the absolute value of the difference between the distance from N_3 to the destination node D and the distance from the neighbor node $N = \{N_1, N_2, N_3, N_4, N_5, N_6, N_7\}$ to the destination node D is not larger than 1, like $|d_{N_3} - d_{N_x}| \geqslant 1, N_x \in N$.

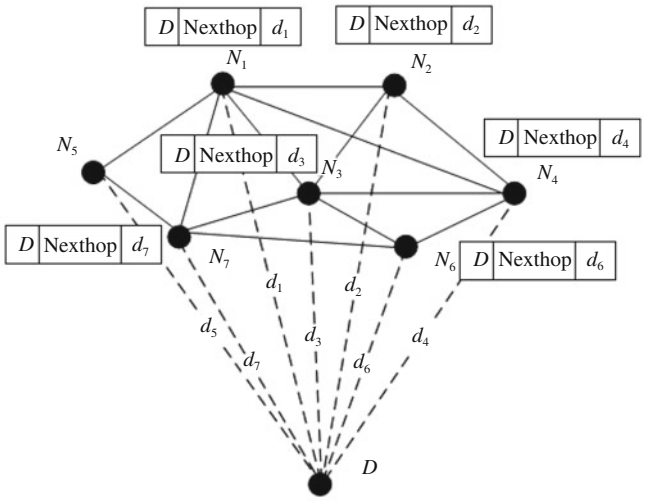

Figure 2 The network topology.

The method of the message correctness verification: when the node N_0 intends to verify the correctness of the routing message (D, N_N, C_M) received from the detection node N_M, it need to perform the comparison according to the following rules:

1) If $C_M = 0$, it is required to verify the prefix of the routing. Actually, the prefix verification is to check if the node has the right to distribute the network address of D (the node is in general bound with the prefix to award the certificate). If it is verified, it indicate that the node is vicious node; otherwise, the information is considered correct.

2) If $C_M > 0$, the following operations are performed:

(i) N_0 fetches the neighbor set $N = \{N_1, N_2, \ldots, N_x\}$ of node N_M according to the maintained data in routing information base (RIB);

(ii) N_0 sends the requests of routing tables to all the nodes in node set N, to request the nodes to send their routing tables to node N_0;

(iii) N_0 gains the distance $C_D = \{C_1, C_2, \ldots, C_x\}$ from the neighbor node set to the destination node D according to the received routing tables and the following comparisons are presented.

3) Fetch (dest_{id}, V_M, nexthop, cost) from RIB, then fetch nexthop= N_y and cost, then fetch (dest_{id}, V_y, nexthop, cost$'$) and verify whether the requirement cost$-$cost$' = 1$ is met. If the requirement is satisfied, it means that the message is false, or continues the following steps.

4) If $C_M = 1$, cost$' = 0$. According to assumption 2), the source of the routing message (dest_{id}, V_y, nexthop, cost$'$) can be know and the integrity of the message can be verified. Thus, it can be considered that the current routing information is correct.

5) If N_M is not the destination node $C_M > 1; \forall C_i \in C_D (i = 1, \ldots, x), C_i \leqslant C_M$, then it can be considered that the message if false. If $C_M > 1; \forall C_i \in C_D (i = 1, \ldots, x), C_i \geqslant C_M$, the message will not be performed any operation to and the algorithm stops. Or the following step continues.

6) Count the number of cases that meet the requirements $C_M > C_i + 1$ and $C_M < C_i - 1 (i = 1, \ldots, n)$. If the number is not larger than T , the routing message is considered to be true; or it is false. T is the security threshold set in the network and it is set according to the demands of the network security. When T is set 1, the network security is high. Nevertheless, it is suitable that T is set 2 or 3 since there may be miscalculation rate when the node computes the forwarding table and the network has certain capacity of intrusion tolerance.

4.3.3 *The effectiveness of the verification method*

Through the analysis of the verification method, the following conclusions can be drawn:

1) Assuming that there is no collusion attack, as long as the node sends a false updating routing message, the false distance sent from it will be inconstant with the updating routing message of the

neighbor node. This implies which means that the message correctness verification method can detect any false updating routing message from the attack nodes.

2) In the prerequisite that the collusion attack exists, the method of the message correctness verification can defend the false routing attack even in some extreme cases. However, it will not influence the performance of other nodes in the network.

4.3.4 *The effectiveness of the verification method*

This subsection analyze the complexity of the proposed message correctness verification method. It is assumed that the average connection degree is β and N is the set of network nodes. When the node intends to verify the correctness of an updating routing message sent from the neighbor node, it needs computing of no more than $(\beta - 1)$ steps. When the node intends to verify the correctness of all the routing messages sent from the neighbor node, it requires computing of no more than $|N| \times (\beta - 1)$ steps. Therefore, the complexity of the correctness of all received messages is $O(|N|)$.

4.4 The verification mechanism of information security

Based on the security rules of distance vector routing protocols, the integrity, freshness and the source verification of routing information need to be guaranteed which ensures the protocols to operate normally. From the routing model of distance vector routing protocols, we know that the routing information is only transmitted between the neighbors. The method of message correctness verification proposed in the last section requires that the node not only gains the routing information of measurement root node, but also gets access to the routing information of the auxiliary trustable node in some case. In addition, the message verification of the auxiliary trustable node is also required so as to achieve the evaluation of the auxiliary trustable.

However, not all auxiliary trustable nodes can exchange routing information with the evaluation nodes. In order to solve the problem, the aggregation signature technology [16–18] is introduced. The mechanism of message verification in distance vector routing protocols is presented as follows and it requires the node to satisfy the following assumptions: 1) the network needs the support of public key infrastructure (PKI), which means that each node has the corresponding public key and private key; 2) each node has the unique network ID which is bound with the prefix of the user network; and 3) the algorithm of public key can support the aggregation signature algorithm.

The verification mechanism of message uses the following notations: T_i represents the current timestamp generated by node i; S_i, P_i stand for the private key and public key respectively; k accounts for symmetric key; $\{M\}key$ represents the cryptogram operation towards the corresponding key using message M; $AggreSig\{M_1, \ldots, M_n\}k$ represents the operation of aggregation signature towards message $M_1, \ldots, M_k$ using the key k; New_Tab_N stands for the latest routing table of node N.

In respect to the network routing, the security certification of routing information can be under two different situations: the transmission of updating routing message and the aggregation routing message. The two above transmission types can be classified as the protection in the PA (packet level) and IA (information level) [11]. The certification of PA is aiming at preventing the updating routing packet from being forged, tamped with and providing the source certification. A provides the protection of PA as well as the confidentiality service of all the routing information in the updating routing packet.

4.4.1 *The transmission of updating routing message*

The transmission of updating routing message means the node only sends its updating routing table to its neighbor node and the neighbor node does not need to verify the correctness of the updating routing message. Actually, the neighbor only needs to conduct the corresponding cryptogram operation in the updating routing table according to the operation level.

$$PA\text{-}1 : MT \longrightarrow MN : Mes = \{T_{MT}, New\_Tab_{MT}\}S_{MT}.$$

Step 1. The node MT sends the current updating routing table to the node MN. The node MT generates a timestamp T_{MN} and uses the private key to sign the integration of T_{MT} and the updating routing table New_Tab_{MT}. Then it sends the signed message to all the neighbor nodes.

Step 2. After the neighbor node receives the message, it will use the public key of the node MT to compute $\{\{T_{MT}, New\_Tab_{MT}\}S_{MT}\}P_{MT}$. If the plaintext message can be gained, the freshness of the timestamp T_{MT} will be checked. If the T_{MT} is fresh, the node MN will believe that the message is not tampered with and forged, but is the latest generated routing table.

For the protection at the IA-level, the node will sign the information $\{T_{MT}, ID_{MN}, New\_Tab_{MT}\}$ and use the public key of the node to encrypt the information. Nevertheless, the nodes are required to establish the symmetric shared key in advance and send the encrypted signature to the node. The sent message is as follows:

$$IA\text{-}1 : N \longrightarrow R : \{\{T_{MT}, ID_{MN}, New\_Tab_{MT}\}S_{MT}\}k.$$

The node needs to use its private key or the symmetric key to decrypt the message which is different from the PA-level protection. Then it uses the public key of the node MT to verify the signature and the remaining verification steps are the same with the operations of the PA-level protection.

4.4.2 *The transmission of the updating aggregation routing message*

After the node MN verify the latest routing table of the node MT generated by the message, if the node MN needs to verify the correctness of the routing table, the PA-level protection node need to interact as the following steps:

$PA\text{-}2 : MN \longrightarrow MT : Req = \{ID_{MN}, ID_{MT}, T_{MN}\}S_{MN}$;

$PA\text{-}3 : MT \longrightarrow MN : AgSi = AggreSig\{T_{MN}, M'_{MT}, M'_1, \ldots, M'_n\}, \{M'_1, \ldots, M'_n\}$;

$M'_i = \{T_{AN}, Tab_i\}S_{AN}, M'_i$ is the signature of updating routing table of the auxiliary trustable node AN_i.

Step 1. When the node MN intends to verify the correctness of the updating routing message sent from the node MT, it sends a verification request which includes the ID of the node MN and MT and the current timestamp. The node MN uses its private key to sign the information and sends it to the destination node MT.

Step 2. The node MT makes the signature computing of the signature message of its current updating routing table and the signature message of the received latest updating routing table from the neighbor node. Then the node MT sends the aggregation signature and the signature message of the latest updating routing tables from all the neighbor nodes to the node MN.

Step 3. The node MN verify the correctness of aggregation signature according to the sent message. If the verification is passed, it is believed that these updating routing tables are the latest routing tables generated by the neighbor nodes of the node MT. Then the correctness of the updating routing message can be performed as the verification methods presented in the Subsection 2.3.

Figure 3 shows the diagram of the information transmission when the nodes RN_1 conducts the information correctness of the node RN_2 in PA level security protection. In terms of the IA-level protection, it is only required to use the public key of the destination node or the symmetric password to encrypt the PA-level protection message.

4.4.3 *The security of the verification mechanism*

1) The security of updating routing message. The timestamp T_{MT} guarantees the freshness of the message. The verification of the signature message guarantees the message integrity. The signature uses the private key owned by the only person so that the source of the message can be verified. Therefore, the current message satisfies the acknowledgement rule of (1) message and the node MN acknowledge the receiving of message Mes.

2) The security of the message transmission in the updating aggregation routing message. According to the information acknowledgement rule of (1), the node MT can acknowledge the receiving of message

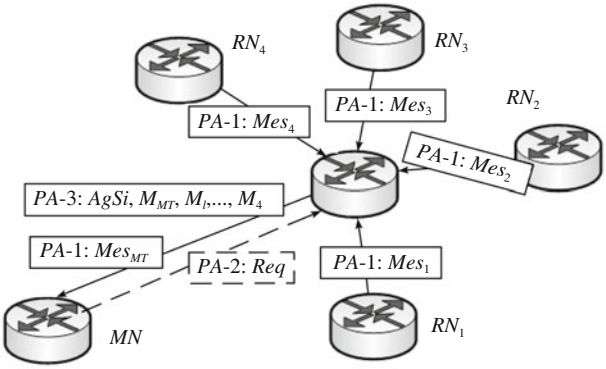

Figure 3 The message delivery of PA level security protection.

Req. Correspondingly, node MN can acknowledge the receiving of $M_i'(i = 1, 2, \ldots, n)$ according to the timestamp, the verification of the signature, the uniqueness of the private key. Also, MN can trust the auxiliary trustable node and believe the correctness of routing information sent by the auxiliary trust node according to the extended auxiliary rules of (4). The aggregation information acknowledges the rule (2) and the node acknowledge the receiving of $AgSi$.

3) The defense against the forgery attack. In the security model, if the cryptogram algorithm is secure and the private key is not revealed, the legal nodes and illegal nodes cannot impersonate other nodes to conduct the attack. The security of the cryptogram infrastructure guarantees that a legal node cannot conduct all kinds of forgery attack.

5 Performance evaluations

5.1 Security analysis

In order to satisfy the trust model, the message correctness verification method and the message security verification mechanism are described in this work. The security mechanism is analyzed as follows.

The transmission of updating routing message satisfies the rule (1) in the security model since the integrity, freshness and certification of the source node are verified.

The mechanism of aggregation signature satisfies the rule (2) in the security model. If a node passes aggregation signature certification successfully, it indicates that. Therefore, the measurement node can judge where the information sent by the measurement root node originates.

The verification mechanism of message correctness satisfies the rule (3) in the security model. The effectiveness of the verification method guarantees that the measurement node can verify the security of the data sent by the measurement root node according to the received data. The verification of the signature information in aggregation signature satisfies the rules (4) and (5) in the security model. The prerequisite of the aggregation signature verification by the measurement node is that the measurement root node trusts its neighbor nodes. Thus, if the measurement node passes the aggregation signature verification, it trusts the correctness of the information received from the neighbor node.

In summary, the security mechanism can meet the requirement imposed by the auxiliary trust model so that it can improve the security of distance vector routing protocols.

5.2 Performance comparison

It is shown in Table 1 that the security mechanism proposed in this paper can meet the security requirement of distance vector routing mechanism. In particular, the false routing attack is the most severe among all the attacks and the mechanism proposed in this paper is the only one that can defend this kind of attacks.

Table 1 The comparison of security performance

Security mechanism	Replay atk.	Forgery atk.	Short-dis atk.	Long-dis atk.	Collusion atk.	Freshness	Mechanism
S-RIP [14]	N	Y	N	N	N	N	MAC function
SDV [15]	Y	Y	Y	Y	N	N	Trust node, public key
Mittal [12]	N	N	Y	Y	N	N	Perception node
Hu [13]	N	Y	Y	N	N	N	Hash function
The mechanism	Y	Y	Y	Y	Y	Y	Public key

Table 2 The impacts of security mechanisms on the network

Security mechanism	γ	ϕ	φ
S-RIP [14]	$k(k+3)$	$k-1$	$k(k+3)(k-1)$
SDV [15]	$2k$	$S-1$	$2k(S-1)$
The mechanism	2	2	2

Table 2 shows the impact of five different mechanisms exerts on the network in the process of message correctness verification. It mainly examines the number (γ) of messages which are required by the nodes participating in the verification, the number (γ) of nodes that are responsible of the verification and the number (ϕ) of messages that are required to be transmitted in the verification each time. It is assumed that the average distance between two nodes in the network is k tops and S accounts for the number of trust nodes that are implemented in the network by SDV.

It is indicated in Table 2 that the strategy presented in this paper exerts the smallest impact on the network. The participants that perform the verification of message correctness are merely the detection nodes and detection root nodes. The reason is that the aggregation signature guarantees the correctness of the auxiliary trust evaluation in the verification methodology proposed in this paper.

5.3 The simulation experiment of the verification method

In this subsection, the simulation tool SSFNet is used to verify the effectiveness of the verification method of the message correctness. The routing protocol adopted to the network is RIPv2. In addition, we assume that the network with 10 Mbps Ethernet interface, the link delay is set to 0.001 s, and the invalid time of link detection on the router is set to 0.02 s. The simulation network topology is generated by BRITE with the maximum connection degree of 30 and the average connection degree of 7.9.

In the simulation scenario, 10 nodes conduct the attack of false routing message. In every routing updating, the 10 nodes are divided into 5 groups and send a false routing message whose distance is 2, 3, 4, 5 and 6 different from the real distance. The security thresholds are set 1, 2, 3, 4 and 5 respectively. The experiment results show that whatever T is set, if the connection degree of neighbor node is larger than T, the detection node is certain to detect the false routing information. However, if T is set 1, there may be some error message, since delay and miscomputing may occur when the network node computes the forwarding table. Therefore, it is suitable that T is set 2 or 3 in order to prevent the the incorrectness of information transmission.

5.4 Memory space

In the security mechanism, the router is required to maintain the up-to-date routing table and the public key certificate received from the neighbor routers. It is assumed that the number of nodes in the network is N, the average number of neighbor nodes is n and the algorithm used in the public key infrastructure is 1024 bit based RSA algorithm. M_{RIB} represents the memory space occupied by routing information database, M_{Cet} accounts for the memory space occupied by public key certificate that is required to be saved. The total memory space occupied is: $M = M_{\mathrm{RIB}} + M_{\mathrm{Cet}} = 20 \times N \times n + 128 \times n \times (n-1)$ bytes. Figure 4 demonstrates the comparison of extra occupied memory space of routers in the proposed security mechanism, Mittal mechanism and RIP mechanism when $n = 4, N = 50, 100, 200, 500$ and 1000 respectively (since Hu mechanism and Mittal mechanism do not occupy extra memory space of nodes,

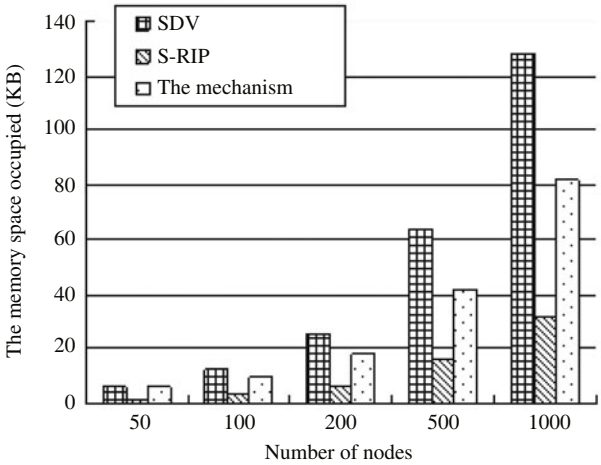

Figure 4 The comparison of memory space requesting.

they are not compared in this paper). It is assumed that SDV uses 1024 bit based RSA algorithm, every node is required to save the public key certificates of all nodes and S-RIP uses MAC function with 256-bit key. It is shown in Figure 4 that the memory space occupied in the strategy proposed in this paper is larger that in S-RIP but smaller than that in SDV. In particular, the occupied memory is 0.082 MB if the number of nodes reaches 1000.

6 Conclusion

Currently, various attacks towards network routers are increasingly popular and the resulted deteriorated and degraded performance become an outstanding and challenging issue needs to be addressed. This paper analyzes the features of distance vector routing protocols and discusses the network attack with false routing information. Based on the analysis, the security goal is presented and the security model and rules are proposed. To well guarantee the freshness, integrity and correctness of the updating routing information, the corresponding security mechanisms are presented. The theoretical analysis and numerical result from simulation experiments demonstrate that the mechanism proposed in this paper can significantly promote and enhance the network security for distance vector routing protocol without introducing significant network overheads and complexity.

Acknowledgements

This work was supported by National Basic Research Program of China (973 Program) (Grant No. 2012CB-315903), National Natural Science Foundation of China (Grant Nos. 61103200, 61070157), and Key Science and Technology Innovation Team Project of Zhejiang Province (Grant No. 2011R50010) .

References

1 Bellovin S.M. Security problems in the TCP/IP protocol suite. Comput Commun Rev, 1989, 19: 32–48
2 Kuo C F, Pang A C, Chan S K. Dynamic routing with security considerations. IEEE Trans Parallel Distrib Syst, 2009, 20: 48–58
3 He L. Recent developments in securing Internet routing protocols. BT Technol J, 2006, 24: 180–196
4 Lakshminarayanan K, Caesar M, Rangan M, et al. Achieving convergence-free routing using failure-carrying packets. In: ACM SIGCOMM 2007. New York: ACM Press, 2007. 241–252
5 Wang B, Guo Y F, Lan J L, et al. Fast network self-healing mechanism based on distance vector routing protocol. J Internet Technol, 2010, 11: 659–667

6 Kim H, Shin G. On predictive routing of security contexts in an all-IP network. Secur Commun Netw, 2010, 3: 4–15
7 Rick K, Simon L, Hart R. Practical interdomain routing security. IT Prof, 2009, 11: 54–56

8 Jun L, Brooks S. I-seismograph: Observing and measuring Internet earthquakes. In: IEEE INFOCOM 2011. Washington: IEEE Computer Society, 2011. 2624–2632
9 Bellman R. On a routing problem. Q Appl Math, 1958, XVI: 87–90
10 Yi Q, James J, David T, et al. Information Assurance: Dependability and Security in Networked Systems. San Fransisco: Morgan Kaufmann Publishers, 2007
11 Haim Z, Levy H. Area avoidance routing in distance-vector networks. In: Proc of IEEE INFOCOM. Washington: IEEE Computer Society, 2008. 475–483
12 Mittal V, Vigna G. Sensor-based intrusion detection for intra-domain distance-vector routing. In: Proc of CCS'02. Washington: IEEE Computer Society, 2002. 127–137
13 Hu Y C, Perrig A, Johnson D B. Efficient security mechanisms for routing protocols. In: Proc NDSS'03. San Diego: IEEE Computer Society, 2003. 1–17
14 Tao W, Kranakis E, Oorschot P. S-RIP: A secure distance vector routing protocol. In: Proc of 2006 Securecomm and Workshops. Washington: IEEE Computer Society, 2006. 103–109
15 Babakhouya A, Challal Y, Bouabdallah M, et al. SDV: A new approach to secure distance vector routing protocols. In: Proc of 2006 Securecomm and Workshops. Washington: IEEE Computer Society, 2006. 1–10
16 Sheng B, Wang H N, Pan J P. Keychain-based signatures for securing BGP. IEEE J Sel Areas Commun, 2010, 28: 1308–1318
17 Neven G. Efficient sequential aggregate signed data. IEEE Trans Inf Theory, 2011, 57: 1803–1815
18 Zhang L, Qina B, Wu Q H, et al. Efficient many-to-one authentication with certificateless aggregate signatures. Comput Netw, 2010, 54: 2482–2491