https://doi.org/10.1051/matecconf/201817303049

Secure routing based on trust model and reference node strategy in Ad Hoc network

Shuiyuan Huan[1,*], *Jianjun Wen*[1]

[1]Chongqing University of Posts and Telecommunications, College of Computer Science and Technology Chongqing Engineering Research Center of Mobile Internet Data Application, Chongqing City 400065,China

Abstract. Ad Hoc network is a kind of wireless mobile network that does not depend on any fixed infrastructure. It has the characteristics of no center, self-organization, and high dynamic and limited energy. Therefore, Ad Hoc network has security risks. The Ad Hoc secure routing based on the trust model and the reference node strategy provides a secure environment for the establishment of communication routing. The AODV routing protocol is improved. The protocol selects a trusted communication node to establish routing according to the comprehensive evaluation result of the trust model, and finds out the data message discarding the attack node by the trust model. At the same time, the reference node strategy is proposed to defend the black hole attack node. Theoretical analysis and simulation results show that the proposed secure routing scheme can effectively detect and isolate malicious nodes, resist black hole attack and data packet attack attacks, and has high security characteristics.

1 Introduction

Ad Hoc network is a wireless mobile network that does not rely on any fixed infrastructure. It has the characteristics of no center, self-organization and high dynamic and limited energy. In the battlefield environment, emergency rescues and mobile conference has a wide range of applications, while its security issues are more prominent, the network is particularly vulnerable to attack capability.

Since there is no fixed infrastructure, mobile Ad Hoc network communication is completely based on wireless communication between nodes. When two nodes are within the communication coverage of each other, they can communicate directly. However, the wireless communication coverage is limited, and two distant nodes need to communicate through multi-hop forwarding of intermediate nodes. In addition, due to the mobility of nodes, the dynamic changes of Ad Hoc network topology need to be based on the multi-hop on-demand routing protocol, that is, routing is established only when there is a data sending request to improve the routing timeliness and reduce unnecessary s expenses. Therefore, Ad Hoc network, the node is both a host and a router, cooperate with each other, and assume the mission of establishing routing and forwarding messages. Normal and healthy communication is based on mutual trust and mutual cooperation among nodes. Once malicious nodes occur to the network, various kinds of security hazards will be caused. The most common ones are data packet discarding attacks and black hole attacks.

2 Related works

The features of the mobile Ad Hoc network (MANET) without infrastructure make them easy to deploy and dynamic. However, the lack of centralized management and monitoring of Ad Hoc networks makes the attack nodes difficult to find. In all security attacks faced by mobile Ad Hoc networks, packet discarding attacks are very common. Malicious nodes actively participate in the establishment of the route after they are trusted by other nodes and exist on normal routes, and discard or discard data packets partially. On the one hand, the source node does not know the packet details and continuously sends data packets, while the remaining nodes cannot detect the loss of data packets, causing the network throughput to decrease and the network delay to increase [2]. For such problems, methods based on multi-path data transmission and neighbor node-based checking methods are proposed. In literature [3], Karlof first proposed selective discarding attack, and used multipath delivery to deal with this attack. And document [4] proposed a dynamic measurement method based on classification nodes. Marti proposed Watchdog algorithm, and the node works in

[*] Corresponding author: 731853165@qq.com

promiscuous mode [5]. The last-hop node uses the feature that the wireless signals is exposed to the air to monitor whether the next-hop node continues to forward the packet. In literature [6], on the premise that malicious nodes do not discard RREQ and RREP packets, a time-based hand-raising penalty strategy is proposed. The black hole attack is that the attacking node fakes and sends a false routing reply (RREP) without understanding the actual routing, and disrupts the normal routing process of the routing protocol [7]. The method of adding a valid bit to the reply message in this kind of attack literature [8], Deshmukh and so on; literature [9] proposed AODV routing protocol based on the trust model. Feifei Bu and others proposed to use the virtual node as the target node to determine the attack node, but the existence of the target node is easily seen by the attack node [10]. The trust evaluation models proposed to [11]. Attack has a certain effect, but for some packet discard attack effect is not obvious.

The routing protocol based on trust evaluation model has the characteristics of small computational complexity, flexible model application and global collection of evidence. In this paper, a secure AODV routing mechanism based on trust model is proposed to message discarding attack and black hole attack.

3 Trust model

The existing trust model is mainly based on the Bayesian approach reference monitor [12] and the vector model reference monitor [13]. The trust model in this paper is based on the Bayesian approach including direct trust and indirect trust, and uses packet-based statistics and time-based statistics the show of hand punishment strategy to assess.

3.1 Message Statistics Strategy Based on Direct Trust Model

Direct trust refers to the trust relationship evaluated by the node by collecting the packet loss rate information based on the packet statistics and the Bayesian trust model. α indicates the number of times the node has a normal packet loss rate and β indicates the number of times that an error has occurred on the node. If the packet loss rate is less than the normal packet loss rate, $\alpha = \alpha + 1$. If the packet loss rate is greater than the normal packet loss rate, then $\beta = \beta + 1$. We use $Direct\_Trust\_value(i)$ to denote the direct trust value of node i.

$$Direct\_Trust\_value(i) = \frac{\alpha}{\alpha + \beta} \tag{1}$$

Aiming at partial data packet discarding attacks, this paper adopts the penalty policy based on packet statistics. This policy needs to modify the format of the original data packet. As shown in Table 1, the numbers of each packet, Num, and the total number of packets, Sum, are added. The original packet information is unchanged.

Table 1. Data message format

Num	Sum	The original message information

During communication, the target node saves a message record table as shown in Table 2, including Routinfor, Lastnum, Lossnum, Rsum and Lossrate. Routinfor represents the node information of the current communication link, lastnum records the number on the last received packet, Lossnum represents the cumulative sum of the packet loss, and Lossrate represents the packet loss rate. As shown in equation (2, 3, and 4):

$$Lossnum = Lossnum + Num - Lastnum \tag{2}$$

$$Rsum = Sum \tag{3}$$

$$Lossrate = Lossnum / Rsum \tag{4}$$

Since there will be a normal packet loss rate on the network, you can set a threshold ρ that is slightly larger than the normal packet loss rate. If Lossrate is greater than the threshold ρ, you can suspect that there are some packets in the path that discard the attacked node. If Lossrate is smaller than the threshold, the path is normal.

Table 2. Node packet record table

Routinfor	Lastnum	LossNumber	Lastsum	Lossrate

3.2 Raising hand reporting strategy based on indirect trust model

Indirect trust refers to the source node collects information reported based on the time hand reporting mechanism and evaluates the relationship through the Bayesian trust model. The Bayesian model under indirect trust evaluation records the reported node and the reported node, and λ indicates the number of times the node is reported or reported. If the node is reported or initiated, $\lambda = \lambda + 1$. We use Indirect_Trust_value (i) to represent the indirect trust value of node i, then (5):

$$Indirect\_Trust\_value(i) = \frac{1}{\theta\lambda + 1} \tag{5}$$

Among them, $\theta(0<\theta<1)$ is the influence factor of indirect trust value, avoiding the indirect trust value dropping rapidly due to multiple reporting.

In reference [5], a hand-raised punishes strategy based on time statistics finds that after a node is attacked, a node initiating a report uses a new message to notify other nodes in the route to end waiting. Considering that a new message has a large overhead, the strategy has been modified, using the normal end of the data packet to inform the end of the node to wait.

Based on the direct trust value and the indirect trust model, the method of calculating the total trust $Trust\_value(i)$ of node i is given, as shown in equation (6):

$$\begin{aligned} &Trust\_value(i) = \eta Direct\_Trust\_value(i) \\ &+(1-\eta)Indirect\_Trust\_value(i) \end{aligned} \tag{6}$$

η is the weight coefficient of the direct trust value, and $0<\eta<1$.

In this paper, by sett a trust threshold F to determine whether a node is credible, greater than F is considered credible, less than F is considered untrustworthy. F is initialized to 0.5, when the trust value of the node is greater than F, the node is considered as trusted; but if the trust value of the node is less than F, the node is considered as untrustworthy.

3.3 Trust value update

Because Ad Hoc network has the characteristics of mobility, it needs regular statistics and updates on trust value of the network. The trust values statistics node and the reference node is the same node.

3.3.1 Initialization

In the network initialization phase, a secure node M is selected as the trust value node and only the time-based punishment mechanism of hand-held report mechanism and the penalty policy based on packet statistics are used during the initial communication. To avoid the exposure to reference nodes, the initialization phase reference node policy does not run temporarily; the initialization trust threshold is set to F.

3.3.2 Trust statistics and updates

The node trusts value and the trust values statistics node periodically updates. Since the attacking node frequently participates in the network communication, the energy consumption of the node is large. The trust value statistical node S performs trust value and remaining energy rate of each node in the network Statistics, for the average trust value below the threshold of the whole network broadcast. At the same time, each node obtains the average trust value information and the attack node information about its own neighbor nodes, and clears the average trust value information about other nodes in the node information table. The trust value is calculated as shown in equation (7):

$$STrust\_value(i) = \frac{1}{n}\sum Trust\_value(i) \tag{7}$$

$STrust\_value(i)$ represents the average trust value of node i.

3.3.3 Reference node update

Considering that the energy consumption of the trust values statistics node S is large, the new trust values statistics node is selected as the node N with the highest trust value and the weighted trust values weighted by the energy residual. To avoid N-node exposure, the update tells the N-node by the S-node. Due to the strong mobility of Ad Hoc networks, N nodes need to reserve a set of candidate nodes, where the candidate node is the node set with the top 10% of the weighted trust values obtained according to (8).

$$\begin{aligned} &WTrust\_value(i) = \mu \times EnergyRate(i) \\ &+(1-\mu) \times STrust\_value(i) \end{aligned} \tag{8}$$

The $EnergyRate(i)$ represents the residual energy rate of the node i, and $WTrust\_value(i)$ represents the weighted trust value of the node i, and the specific value of the weight coefficient of $\mu(0<\mu<1)$ can be determined by the experiment.

3.3.4 Update of path query nodes

It is assumed that the total number of nodes in the network is n, the S node is the reference node and the query node is the node that sends the query message. The point set of the N (trust value statistics node) node randomly selects the point set of the nodes of the weighted 20%-40% before the weighted trust value as the path query node.

$$k = n \times 0.2 \times \gamma \tag{9}$$

4 Secure routing based on trust model

In this paper, secure routing to require that each node maintains a trust table and the trust table is regularly updated according to 3.3.2. The establishment of the security route mainly includes two phases: the reference node policy and black hole attack node discovery, and the establishment of the security route.

4.1 Reference node strategies

Trust-based model often can only prevent data packet discarded attacks, but black hole attacks cannot be a good defense. Therefore, this article further introduces the reference node strategy. Here we set the reference node as S (which is also used as the target node in the reference node strategy), and there are multiple query nodes. As shown in FIG.1, during the path finding message initiated by the source node A, the destination node S receives an RREQ request message from multiple routes. Then, after receiving the RREQ message sent by multiple nodes A, the node S may be sure that node A will send data to it. A node also receives multiple RREP packets, but only the shortest route will be selected. In Figure 1, Node B is a node that attacks black hole hybrid full data packet discard attacks. Therefore, node A chooses the route from node B. After data communication, It is found that the data black hole formed by the node B does not forward the data, and therefore the destination node S cannot receive the data message. Since S knows that node A sends data to it, when node S does not receive data after a period of time, It can suspect that node A has a problem with the current route. Through the report on node S, We can find the attack node.

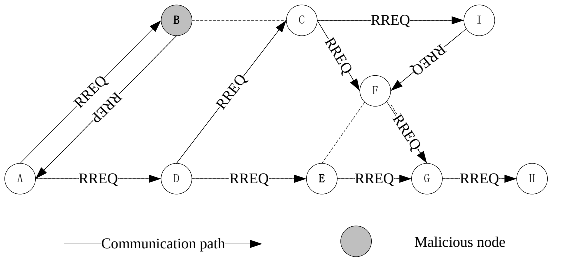


Figure 1. Initiates the routing message process

The reference node S needs to maintain a reference node routing information table when the query node initiates an RREQ packet, as shown in Table 3, including the source node ID, destination node ID, routing link information, and RREQ request start time. This table records a number of routing information about the query node to the reference node. When the node S receives the RREQ packet of the query node A, It immediately sets the time waiting timer, as shown in equation (10).

$$MaxTolerateTime = TolerateWTime + i * a \tag{10}$$

MaxTolerateTime is the maximum tolerable time, TolerateWTime is waiting for tolerance, and i am the number of nodes in the link. The destination node S does not receive the data message from the node an or receives the data message within the MaxTolerateTime time, the S node stops waiting and sends a report message ROUT_SPME (Routing spoofing message), where the format of the ROUT_SPME message is as shown in Table 4, the ROUT_SPME report message includes a message type Type, a destination node ID, a source node ID, and whether or not the data value is accepted. Values of 0 and 1, 1 means that the data is received and 0 means no data is received. When the destination node S sends a report message, it randomly selects a route to the node A for sending from the reference node routing information table.

Table 3. Reference node routing information table

Source ID	Reporter ID	Routinfor	Start_time

Table 4. ROUT_SPME message format

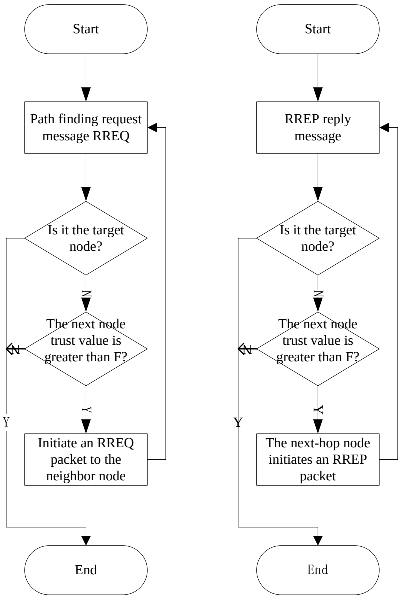
Type	Destination ID	Source ID	Value

When the source node receives the report message from the reference node S, the analysis node receives the ROUT_SPME message information, and if the Type value is 0, queries the current communication route to S and stops the route, queries the returned node B of the RREQ, and sends Node set to attack nodes, the whole network broadcast. If type is 1 this will end the route normally.

In the process, the aforementioned time-based raises hand reporting mechanism and packet-based statistics function normally. When the REPMESS reports message and the ROUT_SPME report messages to exist at the same time, they are handled according to the punishment policy reported by the time-based raise their hands while the report message of the ROUT_SPME is invalid. Because there is a greater chance of attack of discarding completely data packets at this time, Instead of directly judging the node as an attacking node and excluding the network in order to avoid misjudgment choosing lighter penalties.

4.2 Secure routing to find ways

During route routing, the node first determines whether the trust value of the neighbor node is greater than the threshold F before initiating the RREQ packet. If the value is greater than the threshold F, the node sends an RREQ path finding message to the neighbor node; otherwise, the node does not send an RREQ packet, the process shown in Figure 2 (a) below. Similarly, the following nodes will determine the trust value of their neighbors until the target node receives the RREQ packet. After receiving the RREQ packet, the target node initiates an RREP packet of the reverse route. At the same time, the node determines whether the next-hop node trust value is greater than the threshold F according to the flowchart shown in FIG .2 (b) until the destination node receives the RREP or the route one of the nodes is not trusted.


Start
Path finding request message RREQ
Is it the target node?
N
The next node trust value is greater than F?
N
Y
Y
Initiate an RREQ packet to the neighbor node
End
Start
RREP reply message
Is it the target node?
N
The next node trust value is greater than F?
N
Y
Y
The next-hop node initiates an RREP packet
End

a RREQ trust route b RREP trust route

Figure 2. Node path-finding flow chart

The security route determines the trust value of the forward and reverse routes to find a secure route to ensure the security of the communication route.

5 Security analysis

Security analysis is mainly explained from the attack mode of the defense.

5.1 Defense black hole attacks

The reference node strategy is proposed to this paper for the characteristics of the direct forgery of the black hole attack node and the discarding of the data message. The query node initiates an RREQ message to the reference node, and the reference node can receive a request initiated by multiple routes. In this case, the reference node starts the timer; at the same time, the black hole node receives the RREQ message and directly replies to the node with the optimal route, Then inquires the node and the black hole node carries on the correspondence; After all the black hole nodes discard all the packets, the reference node cannot receive any packet information. According to (10) formula, when the timer time exceeds the maximum tolerance time MaxTolerateTime, the reference node initiates the report message ROUT_SPME and Type equal to 1. The source node by viewing the Type information about the ROUT_SPME packet, a black hole attack node can be found and the attack node can be excluded from the network.

5.2 Defense data packet discard attack

The comprehensive evaluation of trust value $Trust\_value(i)$ in trust routing model based on trust model consists of direct trust value and indirect trust value. The direct trust value decreases from the increase in reporting times β . The value of the indirect trust decreases with the increase of the number of λ Times reported; the comprehensive assessment of the trust value and the threshold to compare, you can find out the data packet discarded attack node defense packet discards attacks.

6 Experimental result

In this paper, the ADOV protocol is used as a prototype to deal with packet discarding attacks and black hole attack hybrid full data packet discarding attacks. The security strategy in this paper is simulated and compared.

Simulation platform using Ubuntu 12.04 to build NS 2.35 network simulation platform, experimental simulation part of the fixed environment parameter settings as shown in Table 5:

Table 5. Simulation Parameter Table

Simulation area	1000×300
The total number of nodes	50
Movement type	Random Waypoint
Maximum node speed	20 m/s
Stay time	0s
Number of communication connections	10
Data source type	CBR

6.1 Experiment 1: network delay with the change of communication time.

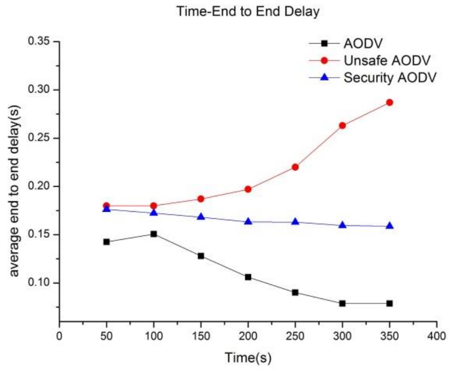


Figure 3. Network average time delay diagram

Figure 3 shows the performance of the AODV routing protocol in terms of end-to-end packet delays in three scenarios of different network conditions. It can be seen that when a malicious node initiates a packet discards attack, the malicious node Discards the message or discards the message partly, the communication breaks down, with the passage of time, and the transmission delay of end-to-end greatly increases. After introducing this scheme, the end-to-end time delay reduces gradually with the passage of time. This is because, once a malicious node initiates an attack, it will be reported by a normal node so as to reduce the trust value. The network periodically cleans malicious nodes. With the passage of time, malicious nodes are easily discovered and removed from network attacks, and the network gradually recovers health. At the same time, since the introduction to this program, each node need to implement the trust statistics and reference node strategy, it will occupy part of the node time, so the network delays is slightly higher than the normal AODV protocol.

6.2 Experiment 2: Packet delivery rate when communication time changes

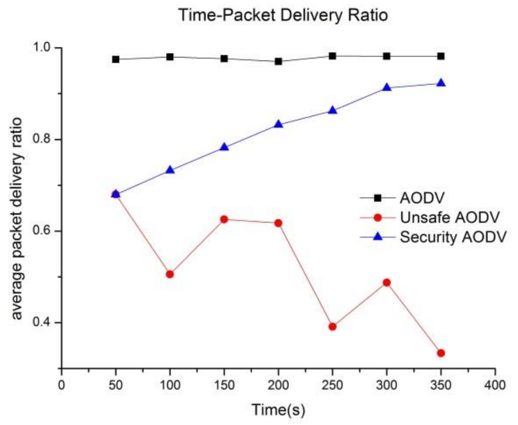


Figure 4. Packet delivery rate in the network

Figure 4 shows the performance comparison of packet delivery rate of three routing protocols. As can be clearly seen from the figure, when an attack node is added, both the black hole attack node and the data packet attack node has packet discarding. Therefore, the node will not receive the message, with the passage of time; the packet delivery rate of the network is getting lower and lower. When the security AODV routing protocol is introduced, since the trust models and the reference node policy can discover and report to attack nodes. As time changes, the attacking node will be gradually discovered and cleared of the network, and the packet delivery rate of the network will be restored to normal.

The experimental results show that the performance of this scheme as the system running time increases. This is because as the malicious nodes become more exposed to time, the system can identify malicious nodes faster and more accurately. At the same time, after introducing this scheme, each node need to implement the trust statistics and reference node strategy, which will increase part of the overhead and increase the network delay.

7 Conclusions

Aiming at the security problems of data packet discarding attacks and black hole attacks existing on Ad Hoc networks and combining the existing defense models, a defense data packet discarding attack and a black hole attacking solution based on trust model and reference node strategy are proposed. Through experimental simulation, the model can detect black hole attacks and data packet discard attacks and improve network security. However, due to the increase of the trust model and the reference node strategy, the delay of the network will be affected. In the next stage, the model will be transplanted to other secure routing protocols and the routing protocol will be improved to reduce the control overhead.

8 References

1. Zhongke Zhan, Yun Wang, A secure communication model for defending against Insider packet dropping attacks, Chinese Journal of Computers. 2003-2014(2010)
2. Karlof, C. Wagner, D. Secure routing in wireless sensor networks: attacks and countermeasures, IEEE International Workshop on Sensor Network Protocols and Applications, 113-127(2003)
3. Haiyan Liu, Liang Tan, Chunling Liu, Improved multi-channel access protocol study based on Ad Hoc, Computer Science, 155-159(2016)
4. S. Marti, Mitigating routing misbehavior in mobile ad hoc networks, International Conference on Mobile Computing and NETWORKING ACM, 255-265(2000)
5. Yanan Song, Study on mobile ad hoc network route security. Doctoral Thesis, Nanjing University of Posts and Telecommunications, (2014)
6. Wang, B. Wei, W. Dinh, H. ET al, Fault Localization Using Passive End-to-End Measurement and Sequential Testing for Wireless Sensor Networks, IEEE Transactions on Mobile Computing. 439-452(2012)
7. Xin Liu, Tantong Zhang. Improved Black hole attack analytical model for MANNETs on demand

routing protocols. Journal of Chongqing University of Posts and Telecommunications. 245-250(2017)

8. S.R. Deshmukh,P.N. Chatur, Secure routing to avoid black hole affected routes in MANET. Colossal Data Analysis and NETWORKING. IEEE,(2016)
9. A. Jain,U. Prajapati,P. Chouhan, Trust based mechanism with AODV protocol for prevention of black-hole attack in MANET scenario, Colossal Data Analysis and NETWORKING, (2016)
10. Feifei Bu,Chunxue Wu, A detection strategy for black hole attack based on AODV, Computer Applications and Software. 273-277(2015)
11. Su Sun, Hong Zhong, Runhua Shi, Yafeng Liu, Secure routing protocol based on trust evaluation in ad hoc network, Computer Engineering, 76-80(2012)
12. S. Buchegger, J.Y.L Boudec, A Robust Reputation System for P2P and Mobile Ad-hoc Networks, Proc of Workshop on the Economics of Peer-to-Peer Systems,(2004)
13. I. Ray,S. Chakraborty, A Vector Model of Trust for Developing Trustworthy Systems. Proc. of European Symposium on Research in Computer Security, 260-27(2004)