Secure Routing Algorithm Based On Trust Value for Ad Hoc Networks

Li Wang, Qingwen Wang and Haijing Zhang

Xi'an Research Institute of High Technology, Xi'an 710025, China

Abstract. The malicious behavior seriously reduce the performance of ad hoc networks. To solve this problem, we propose a secure routing algorithm TLS-DSR. It applies improved the bayesian trust evaluation model to optimize the routing algorithm. The simulation results using network simulator NS-2 demonstrates the algorithm can efficiently resist the betrayed attack and the oscillation attack.

Keywords: Ad hoc networks; Secure routing algorithm; Trust value; Attack.

1. Introduction

Mobile Ad hoc Networks (MANETs) have no fixed infrastructure and it keeps connectivity through mutual cooperation among mobile nodes. Ad hoc networks have no control center. Also, it has a dynamic network topology over completely open wireless channel. Therefore, the stability and the attack-resistant ability are always vulnerable. Now, the security becomes the core problem to be solved for ad hoc networks.

At present, many researchers have proposed various routing mechanisms to improve the security of ad hoc networks, such as the methods based on cryptography or node authentication, which can effectively resist network outside attacks. However, as the emergence of diverse attack means, the “hard protection” does not effectively prevent the types of attack from the internal network. Scholars recently focus on the “soft protection” to reduce the damage, such as the trust-based security routing mechanisms [1-5]. Currently, the attacks of ad hoc inner network include three types.

The first type is betrayal attack in which the malicious nodes suddenly attack the network after accumulating the certain trust value through normal cooperation. The attack action disguised as a normal node is generally difficult to be detected. We only minimize the harm caused by the malicious action.

The second type is oscillation attack. The malicious node swings between the accumulation of trust and abuse of trust in order to maximize the benefit. For instance, the malicious node accumulates the trust value in small transactions and attacks the network in large transactions.

The last type is denial of service attack. While malicious nodes send large amounts of data and packets using the flooding spread network protocol, on the one hand they will consume communication resources of normal nodes. On the other hand, the network has serious congestion as it is full of useless messages based on some flooding routing query mechanism. The efficiency of the network service will be affected due to the congestion.

A dynamic source routing protocol based the trust value (SDSR) is presented in the document [6]. SDSR prevents the denial of service attack. In the protocol the trust model evaluates the node trust value in long term history of cooperation. However, the recent cooperative behavior cannot be effectively evaluated, so the routing protocol is difficult to resist the betrayal attack or the oscillation attack. To solve the problem, this paper presents a dynamic source routing protocol based on the trust values of long term and short term (TLS-DSR). It can effectively resist the betrayal attack and the oscillation attack of dynamic malicious behavior.

2. The establishment of trust model

Trust belongs to the subjective action and it is the each other's judgment based on cooperation experience. Trust itself is not the fact and evidence. The dynamic trust value is gradually evaluated through the constant interaction between the nodes. The assessment can be used to guide the next behavior of the node. Trust has a variety of characteristics such as subjectivity, transitivity, antisymmetric property, dynamic property and so on. The trust value is a quantitative expression of trust, also known as the trust degree and reliability.

2.1 The comprehensive trust value

The Bayesian trust probability model [7] has the better theoretical basis and stronger practicability than the other trust evaluation models. The trust evaluation of adjacent nodes in Bayesian model consists of two aspects, the direct trust assessment and the indirect trust assessment. The direct trust evaluation is based on effective observing the historical behavior and it can be calculated using the empirical Bayesian formula. $T_d(i,j)$ Is the direct trust value for node *i* assess node *j* in formula (1). Node *j* forwards routing packets from node *i*. The number of forwarding success is *s*, and the number of forwarding failure is *f*. The number of observing historical behavior is *n*. *n* is the sum of *s* and *f*.

$$T_d\ (i,j) = \frac{s+1}{s+f+1} \tag{1}$$

If node *j* just enters in the network, the direct trust value cannot be truly expressed due to the lack of historical behavior. Therefore, the confidence is established through other nodes recommending. The indirectly trust value of node *j* is calculated using trust value transfer method. The value will take effect by real detecting deviation degree [8]. Node *i* evaluates the indirect trust of node *j* through node k recommending. $\mathrm{T}_c(i,j)$ is the indirect trust value for node i assessing node j. $T(i,k)$ is the comprehensive trust value for node i assessing node k. $T(k,j)$ is the comprehensive trust value for node *k* assessing node *j*. In formula (2) the indirect trust value is calculated based on trust transitivity.

$$T_c(i,j) = T(i,k) \times T(k,j) \tag{2}$$

The comprehensive trust value $T(i,j)$ for node *i* assessing node *j* is calculated with the direct trust value T_d and the indirect trust T_c in formula (3). The weight of the direct trust is α, which is a continuous number between 0 and 1. α controls the proportion of the direct trust value and the indirect trust value. The size of α is generally decided by the routing assessment policy. Suppose node *j* just enters in the network or changes the location, no direct interaction experienced, the trust is mainly from other nodes recommendation. Then α is very small. With the increasing of node *i* and node *j* interaction, the direct trust proportion is growing. That is, α is also increasing until it is close to 1.

$$T(i,j) = \alpha T_d(i,j) + (1-\alpha)T_c(i,j) \tag{3}$$

Bayesian trust model overlooks an important assessment property. The trust is time-sensitive. It should change over time. The more recent the behavior is, the greater the impact of it on trust value is. Oscillation attack nodes launch a surprise attack after obtaining a positive trust evaluation through good cooperations in the long history interaction. Then the high trust value of long-term historical accumulation will cover recent malicious attacks. So the only long-term trust evaluated system is difficult to detect these malicious attack. This paper introduces the long-term trust value and the short-term trust value, reducing the proportion of history behavior and increasing the weight of recent interactions.

2.2 The long-term and short-term trust value.

The trust value is evaluated based on historical performance of the nodes. The historical period will be divided into multiple parts, and each part is named as a frame. A frame is the minimum quantization to calculate the trust value. The frame time length is not fixed and it can be set based on the current network conditions. If more frequent interactions between the nodes, the time frame can be set short, otherwise it can be set long. The method proposed in this paper is a secure mechanism that the long-term and short-term trust values need to be statisticed, and increasing the weight of short-term trust value. It can effectively prevent sudden attack from dynamic malicious nodes. The short-term trust value is assessed in few time frames (such as one time frame). The long-term trust value is statisticed in multiple time frames (such as *N* time frames).

In a time frame, the trust value is calculated after each interaction between the two nodes and the comprehensive trust value is given. The comprehensive trust value will be constantly updated. The long-term trust value $T_L(i,j)$ is the average value of accumulating the comprehensive trust value of multiple interations in the *N* time-frames. The first calculation formula is (4). $T_L(i,j)$ Can be updeted through the current value and the previous value. The latter calculation formula is (5)

$$T_L(i,j) = \frac{\sum T(i,j)}{N} \tag{4}$$

$$T_L(i,j) = \frac{T_L(i,j)*(N-1)+T(i,j)}{N} \tag{5}$$

The short-term trust value $T_S(i,j)$ for node *i* assessing node *j* is defined in the formula (6). It equals the comprehensive trust value in the current time frame, and the value represents the recent trust relationship of the two nodes.

$$T_S(i,j) = T(i,j) \tag{6}$$

3. TLS-DSR secure routing protocol

TLS-DSR secure routing protocol using the long-term and the short-term trust mechanism is proposed in this paper. The specific routing process is as follows.When packets are transmitted from source node *S* to destination node *D*, a valid route from *S* to *D* is needed. If a valid route meeting the credibility in the current network already has existed, packets can be directly transmitted through the route. If there is no route or the route is no longer valid, source node *S* needs to reinitiate a route discovery process. Node *S* broadcasts a route request (*RREQ*) to its neighbor nodes, the RREQ format is shown in Table 1. *SA* is the *IP* address of the source node. *DA* is *IP* address of the destination node. *seq* is the serial number of route request. *TTL* is the lifetime of the message. *Routelist* records identity informations of all nodes of a valid route. *Tolist* records the overall trust value of nodes.

Table 1 *RREQ* format

SA	*DA*	*Seq*	*TTL*	*T_O list*	*Routelist*

When the neighbor node *A* of node *S* receives *RREQ* packet, it first checks whether the message is received. If it is, node A will ignore the message. If not, the trust table of node *S* evaluation node A is queried. The long-term and short-term trust values of node an are $[T_L(S,A), T_S(S,A)]$ from the table. The overall trust value $T_O(S,A)$ of node *A* is calculated in formula (7). The trust threshold of malicious node is σ. The overall trust value $T_O(S,A)$ is the weight sum of $T_S(S,A)$ and $T_L(S,A)$. The dynamic trust factor $\tau(0\leq \tau \leq 1)$ is introduced in the formula in order to resist the dynamic malicious behavior. The larger τ is, the greater the proportion of the short-term trust value in the overall trust value will be.

$$T_O(S,A) = \tau * T_S(S,A) + (1-\tau) * T_L(S,A)$$
$$\tau = \begin{cases} x, T_L(S,A) - T_S(S,A) \leq \sigma \\ y, T_L(S) - T_S(S,A) > \sigma \end{cases} \tag{7}$$

If the difference between $T_L(S,A)$ and $T_S(S,A)$ is not larger than the threshold value σ $(T_L(S,A) - T_S(S,A) \leq \sigma)$, node *A* is determined to be normal node and the dynamic trust factor τ equals *x*. Otherwise, the difference is more than σ $(T_L(S,A) - T_S(S,A) > \sigma)$, node *A* is suspected to be the malicious node and then the dynamic trust factor τ is adaptively adjusted to *y*. In order to further confirm whether node *A* has a malicious action, *x* must be less than *y*.

If node *A* is suspected to be the malicious node, the dynamic trust factor value *y* will increase the weight of the short-term trust value $T_S(S,A)$. Then the total trust value $T_O(S,A)$ will decrease rapidly, avoiding a sudden attack after the accumulation trust value. This is similar to the system of human credibility. The good reputation getting need longer time than the reputation destruction. In TLS-DSR protocol the dynamic trust factor τ can be dynamically adjusted based on the behavior of the node. When the node with great long-term trust value has a malicious attack, the overall trust value decreases rapidly as τ is adjusted to be larger. The response time of determining malicious nodes will be shorten in the system. Nodes with long-term malicious behavior cannot accumulate the normal trust value in short time, so the mechanism can assist the oscillation attack and the betrayal attack.

If $T_O(S,A) < \sigma$, node *A* will be included in the list of malicious nodes. The network will broadcast the error message RRER to all nodes in the network. Now the other nodes will not receive and forward the packets sent by malicious node *A*. All routes containing node *A* will be canceled.

If $T_O(S,A) > \sigma$, node *A* is judged to be the normal trust node. Node *An* address will be added to the *Routelist* (routing information list). The overall trust value of node *A* is added to *list*. Then node *A* continues to broadcast the updated RREQ message. Repeat the above process to find a trust route to destination node *D*. Then packets can be transmitted from source node *S* to destination node *D*.

4. Simulation and analysis

The simulation is established using NS-2. The direct trust weight α is 0.7 in the calculation formula (3) based on bayesian trust model. Each frame time is 0.025s and N is 20 in the long-term trust value formula. The dynamic trust factor τ is adaptive (x = 0.1, y = 0.7) and the trust threshold σ is 0.5. The main simulation parameters are shown in Table 2.

Table 2 The main simulation parameters

The parameter name	The corresponding value
Simulation area /(m*m)	1500*1500
Simulation duration time /s	100
The total number of nodes	100
The number of malicious nodes	0～25
Flow types	CBR
Packet transmission rate /(packer/s)	8
Packet size / Byte	512
The maximum rate of movement /(m/s)	30
Node communication range /m	250

The system respectively simulate TLS-DSR protocol and SDSR protocol. The packet delivery ratio and routing overhead are the main performance metrics. The simulation results and analysis are given. Fig. 1 shows the packet delivery ratios of the two routing protocols continue to decline with the increasing of the number of malicious nodes. The packet delivery ratio of TLS-DSR is better than SDSR. Fig. 2 shows the routing overhead of TLS-DSR is higher than the one of SDSR.

As TLS-DSR routing protocol takes the long-term and short-term trust mechanism, the advantage is that it can resist a certain degree of betray attack or oscillation attack and the route is more reliable. As a whole, TLS-DSR secure routing protocol with a bit more routing overhead cost can establish a relatively safe and trust route.

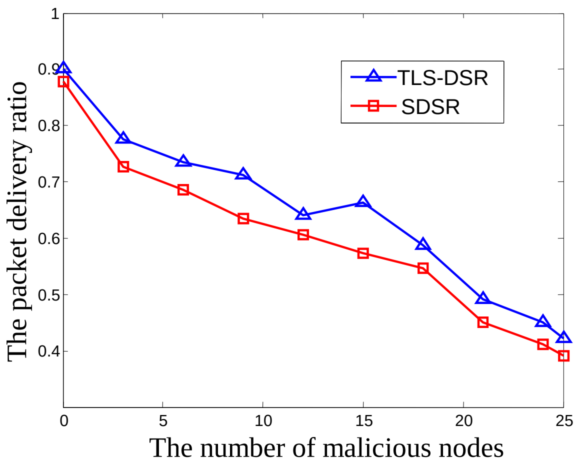

Fig. 1 The packet delivery ratio

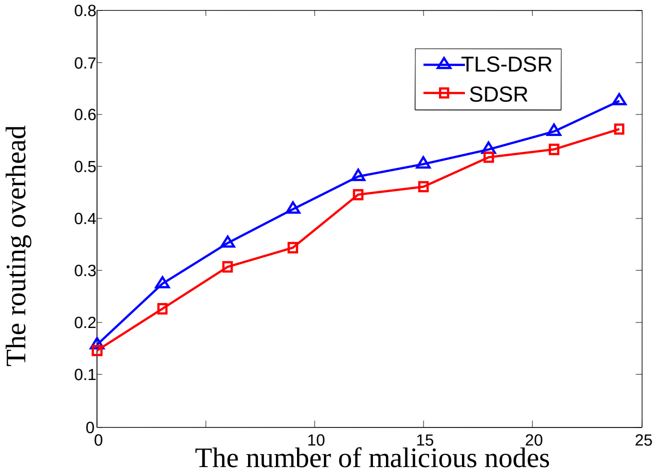

Fig. 2 The routing overhead

5. Conclusion

This paper proposes a dynamic source routing algotithm TLS-DSR. TLS-DSR applies the trust values of long term and short term and improved bayesian trust evaluation model to assist a certain degree of the betrayal attack and the oscillation attack. The simulation results using NS-2 validate the proposed algotithm.

References

[1]. Xu ZJ, Hu Q, Zhang YJ, Ye XM. Trust evaluation routing protocol to enforce cooperation in mobile ad hoc networks, Journal on Communications, 33(7),2012:27-35.

[2]. Zhang F. Node trust evaluation in mobile ad hoc networks based on multi-dimensional fuzzy and Markov SCGM (1, 1) model, Computer Communications, 35(4), 2012:589-596.

[3]. B. Dahill, K. Sanzgiri, B. N. Levine, C. Shields, and E. M. Belding-Royer,” A secure routing protocol for ad hoc networks,”in Proc.ICNP,2002, pp.78-87.

[4]. Y.-C.Hu, D.B.Johnson, and A.Perrig, “Sead:Secure efficent distance vector routing for mobile wireless ad hoc networks,” Ad Hoc Networks, vol.1, no.1,pp.175-192,2003.

[5]. Y.-C.Hu, A. Perrig, and D.B. Johnson, “Ariadne: A secure on-demand routing protocol for ad hoc networks,” in Proc. Mobicom, 2002, pp.12-23.

[6]. Zhang XY, Multi-path dynamic source routing protool based on trust in ad hoc networks, Journal of GanSu LianHe University, 2012, 26(7):50-52.

[7]. Sun YL, Han Z, Liu KJR, Defense trust management vulnerabilities in distributed networks. IEEE Communications Magazine, Feature Topic on Security in Mobile Ad Hoc and Sensor Networks, 2008, 46(2):112-9.

[8]. Sun YL, Han Z, Yu W, Liu KJR. Attacks on trust evaluation in distributed networks. In: Proc. of the Information Sciences and Systems. 2006. 1461-466.