Secure and Authorized Approach Node trust Evaluation in Mobile Ad Hoc Networks

[1]K.Sridevi, [2]M.Sridhar

[1]Assistant Professor Department of Computer Science and Engineering, Muffakham Jah College of Engineering and Technology, Hyderabad, India.

[2]Associate Professor, Department of Computer Applications R.V.R & J.C College of Engineering Guntur, India.

ABSTRACT: *- As Mobile ad hoc networks (MANETs) deployed in adversary environments. There are several routing protocols required to switch data from one node to another but nonetheless they venerable from variety of attacks. Trust model, an abstract psychological perceptive process, is one of the utmost multifarious perceptions in social relationships, concerning factors such as expectations, potentials and activities. All of the above make it problematic to enumerate and estimate trust accurately. In this paper, based on the concepts of fuzzy recognition with feedback, SCGM (1, 1) model and Markov chain, we present a pattern of prediction making.In addition, an efficient trust model is required to handle trust related information in a secure and reliable way.Here, adistributed and efficient trust model was proposed. During the efficient trust model, the calculation of direct trust, commendation trust and indirect trust are deliberated.*

Keywords*—SCGM (1,1) model,Markov chain, Mobile Ad hoc Networks, Trust model*

I. INTRODUCTION

In MANETs, the necessities of anonymouscommunications may be done by way of the mixture ofunindentifiability and unlinkability. Already there are such a lot of anonymous routing protocols proposed. Ourfundamental goal is the form of topology based totally on-demandanonymous routing protocols, which are widespread forMANETs in adversarial environments. The generallyused on-demand ad hoc routing protocols are AODV[2] and DSR . Secure Ad-hoc On-call for DistanceVector Routing Protocol (SAODV) [4] is enhancingversion of AODV routing protocol. SAODV make useof Uneven cryptography with the help of institution signatures. Secure Efficient Ad-hoc Distance VectorRouting (SEAD) [3] protocolis a proactiveroutingprotocol which continues fresh lists ofdestinations and their routes through periodicallydispensing routing tables during the network.This protocol makes use of hash chain technique forchecking the authenticity of the data packet. This hashchainvalue is used for transmitting a routing replace. Both SAODV and SEAD can't satisfythe requirement of anonymous communications. Now,we focus at the MANETs in adverse environments,where the general public and institution key may be to start withdeployed inside the mobile nodes. We advocate anauthenticated anonymous at ease routing (AASR) totriumph over the above troubles.Toauthenticate the RREQ packet at each hop is necessarywhich is achieved by group signature.

The threats which can be particular to MANETS and are as follows: Worm-hole assault, Greyhole assault, Sinkhole assault, and Sybil attack [5-7].Black-hole attack is a kind of lively assault that exploitsthe RREP function of AODV. These assaults involve somemodification of the records flow or the advent of a fakestream [5]. A malicious node sends RREP messageswithout checking its routing table for a fresh path to avacation spot. A RREP message from a malicious node isthe primary to arrive at a source node. Hence, a supply nodeupdates its routing desk for the brand new direction to the precise vacation spot node and discards every other RREP messages from different neighboring nodes or maybe from thereal vacation spot node. Once a source node saves a direction,it starts offevolved sending buffered records packets to a maliciousnode hoping they'll be forwarded to a vacation spot node.Nevertheless, a malicious node (acting a black-hole attack) drops all information packets as opposed to forwardingthem on. A special observe of the various attacks can beseen in [9, 5]. So a ways we realize that black-hole attack is a DoS attack that disrupts the services of routing layer by means ofexploiting the course discovery technique of AODV in MANETS.

II. RELATED WORK

R. Song, L. Korba, and G. Yee, in "AnonDSR: efficient nameless supply routing for mobile ad hoc networks" [7],provided a mechanism in which the anonymous route establishment is predicated upon the quantity of hops among thesource and the destination, time could be expanded as numberof hops will increase, but it lets in the destination nodes to understandall of the intermediate node IDs.

Y. Zhang, W. Lou, and Y. G. Fang, in "MASK:Anonymous On-Demand Routing in Mobile Ad Hoc Networks" [8],proposed an algorithm to offer anonymity which dependson a completely unique type of open key cryptosystem, the pairing-primarily basedcryptosystem, to accomplish unknown correspondence inMANET but it fails on the vacation spot nodes because thevacation spot node ID is found in every RREQ message inundeniable text.

L. Yang, M. Jakobsson, and S. Wetzel, in "Discount anonymous on call for routing for mobile ad hoc networks"[9], proposed the equal machine of ANODR at a decrease cost. Ithas the benefit of carrying out drastically lowercomputation and correspondence complexities at the cost ofexpense of a moderate lessening of safety insurances. Routerequests in Discount-ANODR and in ANODR are parallel howeverthe trouble is that intermediate nodes only recognize thedestination of the request and the identification of the precedingintermediate node but now not the source node.

J. Paik, B. Kim, and D. Lee, in "A3RP: Anonymous and Authenticated Ad hoc Routing Protocol" [10], offerssafety to statistics packets by group signature however the A3RP usedsecure hash feature to calculate the anonymous direction the usage ofthe real IDs of the destination node but it isn't scalable asencrypted onion mechanism.

Author M. J.Probst et.al, 2007 in [13] suggested method that based on observing the neighborsbehavior over thetime.Trust is a fractional valuein [0, 1]. Convergencetime, memory cache requirements are analyzed and some of the merits are mentioned that it can accumulates the past behaviors and weigh thembased on time. Hence thetrust computation is precise. No single point failure.However the complexity in this process is as it requires memoryto store thepast experiments.Computationalcomplexity to determinethe t-distributions.

Authors S. Buchegger et. al,2004 in [14],C. Zouridaki et. al,2005 in [15] described the Past actions andpresent behaviorare combined inBayesian estimateto determine trust.Past actions andpresent behaviorare combined inBayesian estimateto determine trust.And one of the meritis stated that no single point failure. However the complexity in this process is that observation collectionand Bayesian calculations requires memoryand computational complexity.

To review, a lot of work has been completed in trustworthy communications. Trust is naturally determined from a security position grounded on intrusions detected, direct understandings, endorsement from other nodes, charges, etc. Hypothetical models have been proposed and determining trust by analyzing data at the packet level have also been examined.

III. SUGGESTED SYSTEM

Assume the set of the evaluating nodes of the ad hoc network is $\mathbf{A}=\{A_i| \ i=1,2, \ldots,n\}$, the set of attributes of the evaluated node is $\mathbf{B}=\{B_i \mid i=1,2, \ldots,m\}$, where the attribute is such as the transfer speed or signal power etc. Node $A_i$evaluates the attributes of the evaluated node, and the characteristic vector is $a_i=\{a_{1i},a_{2i}, \ldots,a_{mi}\}^T$, so the characteristic matrix set is $\mathbf{D}=(a_{ij})_{m\times n}$.

In order to overcome the influence of different dimensions, we change the characteristic matrix into the standard matrix as $\mathbf{R}=(r_{ij})_{m\times n}$, where $r_{ij} = (a_{ij} - a_{imin}) / (a_{imax} - a_{imin}$and a_{imax} is the maximum of the i-th attribute, a_{imin} is the minimum of the i-th attribute. Assume the attribute weight vector is given by$\mathbf{W}= \{w1, w_2, \ldots, w_m\}^T$, where $w_i \geq 0$, $\sum_{i=1}^{m} w_i = 1$.

Then the combined attribute value of the evaluated node by the j-th evaluating node is computed by the following formula:

$$Z_i = \sum_{i=1}^{m} w_i r_{ij} \qquad (1)$$

According to formula (1), after computing the combined value, we acquaint a vector **Z**:

$$\mathbf{Z} = \{ z_1, z_2, \ldots, z_n \} \qquad (2)$$

A. Compute the Fuzzy Classification of the Combined Value

The formula (2) can be regarded as the single index of fuzzy classification for the set of evaluating nodes. Assume the set of evaluating nodes is classed into c types, such as "bad", "generic", and "good". The

corresponding fuzzy recognition matrix can be expressed as follows:

$$\mathbf{U} = (\mathrm{uhj})_{c\times n} \quad (3)$$

where u_{hj} is the relative membership which the j-th evaluating node belongs to the h-th type, and formula (3) should suit the following condition:

$$\sum_{h=1}^{c} u_{hj} = 1 \quad (4)$$

Assume the attribute of h type character values is the center of h type, the fuzzy cluster center as the following matrix:

$$\mathbf{S} = (s_{ih})_{m\times c} \quad (5)$$

where $0 \le s_{ih} \le 1$。

In order to solve the optimized fuzzy recognition **U** and the optimized cluster center **S**, we establish the object function where the sum of the weighting Haiming distance square between evaluating node set and all types are minimum.

$$\min\{F = \sum_{j=1}^{n}\sum_{h=1}^{c}\{u^{2}{}_{hj}\sum_{i=1}^{m}[w_i(r_{ij} - s_{ih})]^2\}\} \quad (6)$$

In details, the computation process can be listed as follows according to formula (6).

①: If the optimized cluster center **S** and weight vector **W** are given, solve the optimized fuzzy recognition **U**.

$$\min\{F(u_{hj}) = \sum_{j=1}^{n}\sum_{h=1}^{c}\{u^{2}{}_{hj}\sum_{i=1}^{m}[w_i(r_{ij} - s_{ih})]^2\}\} \quad (7)$$

According to the object function (7) and formula (4),we create the Lagrange function and let derivative be zero, as follows:

$$L(u_{hj}, \lambda) = \sum_{j=1}^{n}\sum_{h=1}^{c}\{u^{2}{}_{hj}\sum_{i=1}^{m}[w_i(r_{ij} - s_{ih})]^2\} \quad (8)$$

$$-\lambda(\sum_{h=1}^{c} u_{hj} - 1)$$

$$\frac{\partial L(u_{hj}, \lambda)}{\partial u_{hj}} = 2u_{hj}\sum_{i=1}^{m}[w_i(r_{ij} - s_{ih})]^2 - \lambda = 0 \quad (9)$$

$$\frac{\partial L(u_{hj}, \lambda)}{\partial \lambda} = \sum_{h=1}^{c} u_{hj} - 1 = 0 \quad (10)$$

According to formula (9) and (10), we get the following results:

$$u_{hj} = \left[\sum_{k=1}^{c}[\sum_{i=1}^{m}[w_i(r_{ij} - s_{ih})]^2 / \sum_{i=1}^{m}[w_i(r_{ij} - s_{ik})]^2\right]^{-1} \quad (11)$$

Obviously, if the standard matrix **R**, the optimized cluster center **S** and weight vector **W** are known, we can get the optimized fuzzy recognition **U** from formula (11).

②: If the optimized fuzzy recognition **U** and weight vector **W** are given, we solve the optimized cluster center **S**.

$$\min F(s_{ih}) = \sum_{j=1}^{n}\sum_{h=1}^{c}\{u^{2}{}_{hj}\sum_{i=1}^{m}[w_i(r_{ij} - s_{ih})]^2\} \quad (12)$$

$$\frac{\partial F(s_{ih})}{\partial s_{ih}} = 2\sum_{j=1}^{n} u^{2}{}_{hj}w^{2}{}_{i}s_{ih} - 2\sum_{j=1}^{n} u^{2}{}_{hj}w^{2}{}_{i}r_{ij} = 0 \quad 13)$$

$$s_{ih} = (\sum_{j=1}^{n} u^{2}{}_{hj}r_{ij}) / (\sum_{j=1}^{n} u^{2}{}_{hj}) \quad (14)$$

Obviously, if the standard matrix **R**, the optimized fuzzy recognition **U** and weight vector **W** are known, we can get the optimized cluster center **S** from formula (14).

③: If the weight vector **W** is given, solve the optimized fuzzy recognition **U** and the optimized cluster center **S**.

According to formula (11) and (14), by using of circular calculation, the optimized fuzzy recognition **U** and the optimized cluster center **S** can be computed.

Assume the source nodeof the ad hoc is **SN** (source node, in section 3, it may be node $\mathbf{A}_i$), and **NN** (new node) is the new node in the link route of the **SN**. The set of attributes of the **NN** is $\mathbf{B}=\{B_i \mid i=1,2, \ldots,m\}$, where the attributes are defined in the section 3. Node **SN** records the series time data based on **B** in the nearest time, so the characteristic vector is $tb_i=\{tb_{i1}, tb_{i2} \ldots, tb_{im}\}$, where$i$ denotes time break. And the characteristic matrix set is $\mathbf{TB}= (tb_{ij})_{n\times m}$.

In order to overcome the influence of different dimensions, the characteristic matrix**TB** is changed into the standard matrix denoted $\mathbf{TBR}=(tbr_{ij})_{n\times m}$. At time i, source node **SN** can compute the trust reliability with matrix **TBR**. Assume the attribute weight vector is$\mathbf{W}=\{w_1, w_2, \ldots, w_m\}$, where $w_i \ge 0$,In order to overcome the influence of different dimensions, the characteristic matrix**TB**is changed into the standard matrix denoted $\mathbf{TBR}=(tbr_{ij})_{n\times m}$. At time$i$, source node **SN** can compute the trust reliability with matrix **TBR**. Assume the attribute weight vector is$\mathbf{W}=\{w_1, w_2, \ldots, w_m\}$, where $w_i \ge 0, \sum_{i=1}^{m} w_i = 1$.Then the combined attribute value of **NN** node at the time iis computed as follows:

$$X^{(0)}(i) = \sum_{j=1}^{m} w_j tbr_{ij} \quad (15)$$

According toformula (15), we can get the original index series of trust reliability value, which generates the following vector:

$X^{(0)} = \{x^{(0)}(1), x^{(0)}(2), \ldots, x^{(0)}(n)\}$ (19)

=1. Then the combined attribute value of **NN** node at the time iis computed as follows:

$$X^{(0)}(i) = \sum_{j=1}^{m} w_j tbr_{ij} \quad (16)$$

According toformula (16), we can get the original index series of trust reliability value, which generates the following vector:

$X^{(0)} = \{x^{(0)}(1), x^{(0)}(2), \ldots, x^{(0)}(n)\}$ (17)

$X^{(0)}$ is the non-negative original trust reliability data sequence. The accumulated generation operation of the original data sequence is defined as

$X^{(1)} = \{ x^{(1)}(k) | x^{(1)}(k) \geq 0, k=1,2,\ldots,n \}$ (18)

where $x^{(1)}(k) = \sum_{i=1}^{k} x^{(0)}(i)$.

B. Markov process model

The importance of grey SCGM (1, 1) model is that exponential curve is used to fit original trust consistency value data and geometry graph of the results is a smooth curve. As trust reliability value is a dynamic character value, and time series data have biggish volatility, the change trend is non-stationary stochastic process, so the single application of grey SCGM (1, 1) model influence the precision of the transformed results. Markov chain is a kind of stochastic process without aftereffect, which describes stochastic phenomenon: the present state is aware, and the probability distribution of the future state has nothing to do with the past state. The Markov chain, state transition probability is used to reflect the influence degree of the stochastic factors. Therefore, we can apply Markov chain to make time original series data that have biggish stochastic volatility precise.

C. Trust algorithmmethodology

The suggested algorithm is based on the trust values ofindividual nodes. Initially, allthe nodes of wireless ad-hoc network have zero trust value. The algorithm comprises the following steps:

• **Initialization**:

Trust values of all the participating nodes are initializing with zero.

Initialize the threshold value of the trust value with 100.

Assumption: 1 trust value = 10 packets dropped.

Updating of trust values:

Step1. If the packets are correctly transmitted from one node to another node:

a. If the correctly transmitted number of packets is between 1 to 10, then trust values of the respective nodeswill be incremented by one time.

b. Updated trust value = old trust value + 1;

c. If the correctly transmitted number of packets are greater than 10, then the updated

d. trust value will be:

e. Updated trust value = old trust value + (correctly transmitted packets / 10);

Step2. If the packets are dropped/delayed :

a. The number of dropped or delayed packets is between 1 to 10, then trust value of that particular node isdecremented by one.

b. Updated trust value = old trust value – 1;

c. The number of dropped or delayed packets are greater than 10, then trust value of that particular node will be Updated trust value = old trust value – (Packet dropped or delayed / 10);

Step3. If the trust value of particular node is negative, then print "Invalid node".

Isolating the Packet drop node from the network:

If (Updated trust value <<< Threshold trust value)Then the particular node is treated as malicious node (Black hole node)

If (Updated trust value > Threshold trust value) Then the particular node is treated as legitimate node.

Stop comparing the trust values of nodes with threshold value.

In our approach, we detect the black hole node based on the trust values (Proposed trust value algorithm). We usedTraffic pattern Analysis Techniques and associate trust values with each wireless nodes. Initially, all nodes has 'zero'trust value. If the particular node is not involving in packet drops, then each time the trust value of corresponding nodewill increase by 1.

IV. SIMULATION RESULTS

In a mobile ad hoc network grounded on the 802.11b companionable devices, the existent throughput can be only half of the ideal bandwidth it should be, that is approximately 0.1Mbps to 1.5Mbps. In an actual environment, the working distance for 802.11b is 300m, and working at a distance more than 150m will be regarded as instable speed. Based on this

principle, we can draw that a speed of 0.5Mbps (63KB/s) is good reliable, and 2Mbps (250KB/s) is generic.

Four nodes are available for assessment and the attribute value for each node is in the table I.

Node	Package losing rate (%)	Transmission Speed(KB/s)	Signal1 0^{-7}mW	Signal changing Rate dBm/s
A1	24	260	1.2	2.21
A2	82	70	0.4	2.51
A3	11	290	1.45	3.32
A4	36	298	3.41	2.14

In this determination, we have exasperated to evaluate the superior effects of the Packet Drop attacks in the Wireless Ad-hoc Networks. To attain thiswe have replicated the wireless ad-hoc network set-up which contains packet drop node using NS2 Network Simulator program. Tocreate the packet drop node in a wireless ad-hoc network we have working fresh protocol that hedge down data packets after be amagnet for them to itself.

Simulation Used	NS-2.32
Number of Nodes	50,60,70,80,90,100
Dimension of Simulation Area	1000 * 1000
Routing protocol	AODV
Simulation Time	100sec
Antenna Type	Omni Antenna
MAC Protocol	IEEE 802.11
Queue	DropTailPriQueue
Channel Type	Wireless Channel
Packet Size	152 te

V. CONCLUSION

Despite the fact scheming a new trust system, it is mandatory to contemplate the constraints and the type of data that can beused as input by the network. In this paper, we have presentedan algorithm of assessing node trust on the base of the Markov SCGM (1,1) model is also presented in this paper. It syndicates grey system model with Markov chain. The algorithm not only the evidence that is obtained by past data can be fully used, nonetheless also can measure similarity degree of random length analogous series efficiently, and can deal with with non-stationary time series, avoid the influence of time series data that have biggish stochastic instability to mining precision, so it has preferable practicability. Based on the two models, the analysis and above trust valuationsample shows that the models can be applied to the trust assessment for nodes in mobile ad hoc network.

REFERENCES

[1] Devesh Kumar Pal et al, “Survey on Security Issues in Mobile Ad HocNetworks”, IJCSIT (2014.

[2] Sheng Liu, Yang, Weixing Wang, “Research ofAODV Routing Protocol for AdHoc Networks”, 2013AASR, Conference on Parallel and DistributedComputing and Systems.

[3] Prasuna V. G, Dr. S. Madhusudhana Verma,“SEAD-FHC: Secure Efficient Distance Vector Routingwith Fixed Hash Chain length”, Global Journal ofComputer Science and Technology Volume 11 Issue 20Version 1.0 December 2011

[4] C. Sreedhar, Dr. S. Madhusudhana Verma, Dr. N.Kasiviswanath, “Performance Analysis of SecureRouting Protocols in Mobile Ad-Hoc Networks”,International Journal of Computer Science andTechnology.

[5] M. Imani, M. E. Rajabi, M. Taheri and M. Naderi, “Vulnerabilities in Network Layer at Wireless Mesh Network(WMNs),” Proceeding from ICENT’10: 2010 International Conference on Educational and Network Technology, Qinhuangdao, 25-27 June 2010, pp. 487-492.doi:10.1109/ICENT.2010.5532257

[6] F. Nait-Abdesselam, B. Bensaou and T. Taleb, “Detectingand Avoiding Wormhole Attacks in Wireless Ad-HocNetworks,” IEEE Communication Magazine, Vol. 46, No.4, 2008, pp. 127-133. doi:10.1109/MCOM.2008.4481351

[7] V. Zhang, J. Zheng and H. Hu, “Security in WirelessMesh Networks,” Auerbach Publications Taylor & Francis Group, London, 2009

[8]http://www.freepatentsonline.com/7093133.html (Last usedon 9/4/2013)

[9] S. Dokurer, Y. M. Erten and E. A. Can, “Performance Analysis of Ad-Hoc Networks under Black Hole Attacks,” Proceeding from SECON’07: IEEE Southeast Conference, Richmond, 22-25 March 2007, pp. 148-153.

[10] Hwan-Seok Yang, Seung-Jae Yoo “Authentication Techniques for Improvingthe Reliability of the Nodes in the MANET”, IEEE (2014)

[11] S.S.Zalte, Prof.(Dr.) Vijay R.Ghorpade, “Secure Token for Secure Routing ofPacket in MANET”, IJCSIT(2014)

[12] Miss Morli Pandya, Associate Prof. Ashish Kr. Shrivastava, “Review onsecurity issues of AODV routing protocol for MANETs”, IOSR Journal ofComputer Engineering (2013)

[13] M. J. Probst and S. K. Kasera, “Statistical trust establishment in wireless sensor networks,” in Proceedings of the 13thInternational Conference on Parallel and Distributed Systems, pp. 1–8, 2007.

[14] S. Buchegger and J. L. Boudec, "A robust reputation system for P2P and mobile ad-hoc networks," in In Proc. 2nd Workshop on Economics of Peer-to-Peer Systems, 2004.

[15] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "A quantitative trust establishment framework for reliable datapacket delivery in MANETs," in SASN '05: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensornetworks, pp. 1–10, 2005.