IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Finding Trusted Node in Mobile Ad-Hoc Network

G.Viswanathan[1*], M. Jayakumar[2]

[1] Department of Computer Technology, SNMV College of Arts and Science, Coimbatore, Tamil Nadu, India
[2] Department of Information Technology, SNMV College of Arts and Science, Coimbatore, Tamil Nadu, India

Corresponding Author: gviswanathanphdscholar@gmail.com, Tel.: +91-9600499943

DOI: https://doi.org/10.26438/ijcse/v7i5.684689 | Available online at: www.ijcseonline.org

Accepted: 25/May/2019, Published: 31/May/2019

***Abstract*—**The mobile ad hoc networks (MANETs) encompassed of a dynamic topology and open wireless medium may lead to MANET affected by several security liabilities. MANET could be set of restricted vary wireless nodes that perform in a cooperative manner thereby increasing the overall range of the network. The performance of ad hoc networks depends on the supportive and trust environment of the distributed nodes. To enhance security in ad hoc networks, it is important to evaluate the trustworthiness of alternative nodes without centralized authorities. In this paper, a study was made based on the trust models such as direct Trust, Indirect Trust and Analytic Network Process (ANP). These trust models are incorporated to reflect the trust relationship's complexity and uncertainty. Based on the trust factors, the selection of the trusted nodes is obtained by using methods like direct Trust, Indirect Trust, and Analytic Network Process. ANP is used for making trust decisions which replace the traditional methods like direct Trust and Indirect Trust methods. Hence from the study, we analyzed that the selected nodes obtained by using the ANP decision theorem eliminate the malicious nodes and helps to protect the network from any internal attacks.

***Keywords*—**MANET, Trusted Node, Direct Trust, Indirect Trust, Analytic Network Process.

I. INTRODUCTION

An Electronic network, additionally mentioned as an information network, could be a series of interconnected nodes which will transmit, receive and exchange knowledge, voice and video traffic. Network devices use a spread of protocols and algorithms to specify precisely however endpoints ought to transmit and receive information. For example, the Ethernet standard establishes a common language for wired networks to communicate, and the 802.11 standard does the same for wireless local area networks (WLANs).

An ad hoc network may be a network composed of individual devices act with one another directly. The term implies spontaneous or unplanned constructions. As a result of these, networks usually bypass the gate keeping hardware or central access purpose like a router. Many unplanned networks area unit enable native space networks wherever computers or alternative devices area unit enabled to send information on to each other instead of rummaging a centralized access purpose.

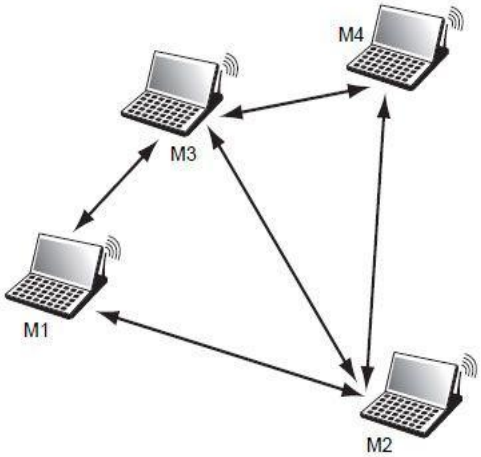

Figure 1: Ad-hoc Network

Mobile ad-hoc networks i.e. MANET are autonomous and non-centralized wireless technology. MANETs involve mobile nodes that allows area unit free in shifting in and go into the network. Nodes area unit includes the techniques or Gadgets, that is, Cell phone, Laptop Computer, individual Electronic Devices, MP3 player, and PC that are forming the network and are mobile.

These nodes will work like host/router or each at a similar time. They can form irrelevant topologies based on their connection with each other in the network. These nodes have the aptitude to line them up, and sense of their self-settings capability. They will be enforced quickly while not the necessity for any infrastructure.

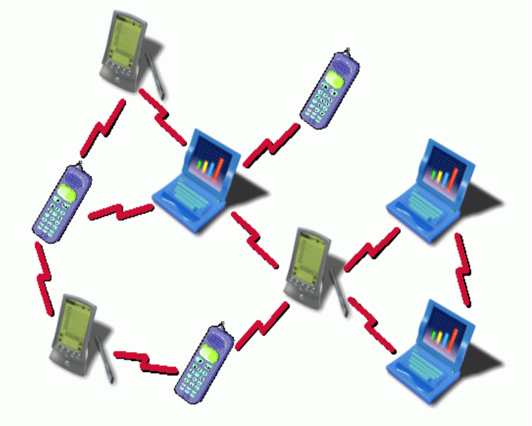

Figure 2: Mobile Ad-hoc Network

II. LITERATURE REVIEW

Although there has been substantial work on trust management models [16], their applicability in mobile agent systems has received limited research attention. In a venture to improve the integrity of utilizing suggestions, Li et al in [1] take a confidence term in their assessment by consolidating two things: confidence and trust combined to form trustworthiness. They use the trustworthiness data to give mass on recommendations in which more weight age is given to the suggested node with higher trustworthiness. Collusion attack gives bad suggestions which are not considered in this work, and they may origin mistaken assessment of the accepted suggestions. Authors in [2] offered RFS Trust, a trust model in view of fuzzy recommendation resemblance, that is exhibited to measure and assess the dependability of nodes. They utilize a similarity hypothesis to assess the suggested connections within nodes. Higher the value of resemblance between the evaluating and the suggested node, the more predictable is the computation within two nodes. In this structure, just a single kind of circumstance is examined that is a selfish node attack and the execution of the structure isn't tried against different attacks identified with endorsement.

The model can detect malicious nodes only if there are few in the numbers and also it utilized Analytic Hierarchy Process (AHP) [3] to set up a hierarchical skeleton within which multi-attribute decision problems can be structured to determine the weight for the trust factors. Yet, the strict hierarchical structure might have to be relaxed once modeling a lot of sophisticated decision problem that involves interdependencies between elements of a similar cluster or completely different clusters.

In the subjective trust evaluation model proposed in the [4] uses the credibility of nodes can be evaluated using the analytic hierarchy process theory and fuzzy logic rules prediction method. In the model established by Sun et al. [5, 6], trust is measured by entropy. They introduced an entropy function to represent the trust value between two nodes, which really captured the dynamic nature of trust evidence. To compute the indirect trust value, both George and Sun's models used trust value iteration techniques considering multi-level directed graph. When more nodes are involved, the convergence speed of this scheme is exponentially slow, and its flexibility becomes a big challenge.

A trust management model was proposed by Josang [7] based on the subjective logic model, which introduced the evidence space and the conception space to describe and measure the concept of trust relationships. This model defined a set of subjective logic operators for the derivation and comprehensive calculation of trust value. Beth et al. [8] proposed a trust management model, which introduced the concept of experience to express and measure trust, in which the credibility formula was derived and integrated. This model is divided into direct trust and recommendation trust which was used to describe the trust relationship, respectively, between the subject and object, subject and recommendation object. Yu et al. in [9] propose a clustering procedure for separating reliable suggestion from unreliable ones. They focus on the predominance law by choosing the cluster with the maximum number of suggestion as a reliable one. Bad mouthing and ballot stuffing attack were demonstrated by this system. On the other hand, predominance law could not be in favor because of conspiring node and not deliver a correct opinion about other nodes. A recommendation exchange protocol (REP) is proposed by Pedro B. et al. [10] to enable nodes to send and receive recommendations from neighboring nodes. It presents the idea of relationship maturity in view of to what extent nodes have known one another. Recommendations sent by long term associates are weighed higher than that from short term associates. The maturity of the relationship is assessed based on a single factor by considering just the duration of the relationship.

Hermes [11] is a recommendation based trust structure which introduces a concept that is the acceptability threshold. The thought of holding ability is utilized in the calculation of recommendation to verify that sufficient examination of the behavior of engaged node has been acquired. Yet the process of intelligibility is a trade-off between getting more close trustworthiness value and time needed to acquire it.

III. APPLICATIONS OF MANET

Some distinctive MANET applications include:

- **Military field:** Ad-Hoc networking allows the army to take advantage of the good thing about typical network experience for conserving any data network among vehicles, soldiers, and headquarters of knowledge.
- **Cooperative work:** To facilitate the industrial settings, the necessity for united computing is extremely important external to the workplace atmosphere and surroundings as compared to the inner setting. People wish to obtain outside conferences for exchanging the data and cooperating with one another concerning any assigned task.
- **Confined level:** Ad-Hoc networks are able to freely keep company with immediate, in addition, momentary hypermedia network by means of laptop computers for sharing the info with all the contestants e.g. classroom and conference. The additional valid and confined level application could also be in domestic network wherever these devices will interconnect straight in exchanging the data.
- **PAN and Bluetooth:** A PAN is localized and small vary network whose devices usually belong to such as an individual. Limited-range Manet-like Bluetooth will build easier the exchange among many moveable devices sort of a portable computer, and a cell phone.
- **Business Sector:** Ad-hoc network may well be used for rescuing and emergency processes for adversity help struggles, for instance, in flood, fire or earthquake. Emergency saving procedures ought to come about wherever broken and non-existing transmissions structure and fast preparation of transmission networks are needed.
- **Sensor Networks:** Managing home appliances with MANETs in both the cases like nearby and distantly, Tracking of objects like creatures and Weather sensing related activities.
- **Backup Services:** Discharge operations, tragedy recovery, analysis or status or record handling in hospitals, alternate of stationary infrastructure.
- **Educational sector:** Arrangement of communications facilities for computer-generated conference rooms or lecture rooms or laboratories.

IV. CHALLENGES OF MANET

- **Limited Bandwidth:** The wireless networks have a restricted information measure as compared to the wired networks. Wireless link has a lower capability as compared to infrastructure networks. The effect of fading, multiple accesses, interference condition is very low in Ad-hoc networks in comparison to the maximum radio transmission rate.
- **Dynamic topology:** Due to dynamic topology the nodes have less trust between them. Some settlement area unit is found between the nodes and then it conjointly builds trust level questionable.
- **High Routing:** In Ad-hoc networks because of dynamic topology some nodes changes their position that affects the routing table.
- **The problem of Hidden terminal:** The Collision of the packets area unit control is observed because of the transmission of packets by that node that doesn't seem to be within the transmission mechanism vary of sender aspect however area unit is in range of receiver side.
- **Transmission error and packet loss:** By rising in collisions, hidden terminals, interference, simplex links and by the quality of nodes frequent path breaks a better packet loss has been featured by Ad-hoc networks.
- **Mobility:** Due to the dynamic behavior and changes within the configuration by the movement of the nodes, Ad-hoc networks face path breaks and it also changes in the route frequently.
- **Security threats:** New security challenges are brought out by Ad-hoc networks because of its wireless nature. In Ad-hoc networks or wireless networks, the trust management between the nodes results in the many security attacks.
- **Power-constrained and operation:** This is conjointly thought-about as a challenge for the Edouard Manet network. The MANET is a network where all nodes rely on the batteries or some exhaustible source of energy. Conversion within the energy is the optimized criteria and a crucial system style. Lean power consumption is also used for lightweight mobile terminals. Conservation of power and power-aware routing is another facet that should be thought about.
- **Security and Reliability:** Nasty Neighbor relaying packets is also a security problem along with other vulnerabilities connected. Dissimilar schemes are used for authentication and key management in scattered operations.

V. IDENTIFICATION OF TRUSTED NODE IN MANET

In this paper, a traditional trust management models and Analytic Network process models were studied to select the trusted nodes which exclude the malicious nodes in order to establish secure communication. The trust [15, 16] Model factors are obtained and it includes Direct Trust, Indirect trust, and Analytic Network Process.

Direct Trust: One of the most important aspects of trust management schemes is the process of data collection for trust calculation. The Direct Trust estimation of a neighbouring hub can be determined by the distinctive trust measurements of that specific hub on various occasions happened in the system. The trust metrics, i.e. the QoS characteristics that can be taken into account. The DT is also one of the functions of trust metrics. The listed trust metric data for different events are essential and can provide useful feedback to the system, towards the proper decision making by the trust management system in the node. Here, contingent upon the application, we can demand the base dimension (limit) to all the trust measurements, or we can have various edges to various gatherings of trust measurements. When one or more trust metric edges are fixed, our trust management framework thinks that no hub is believed except if it is having the least limit level in a given trust metric carefully. This is the principle preferred position of our proposed trust management model contrasted with other different models. Also, this is the place our proposed Trust Evaluation model channels the malicious and selfish hubs in taking an interest in the packet steering in WSN.

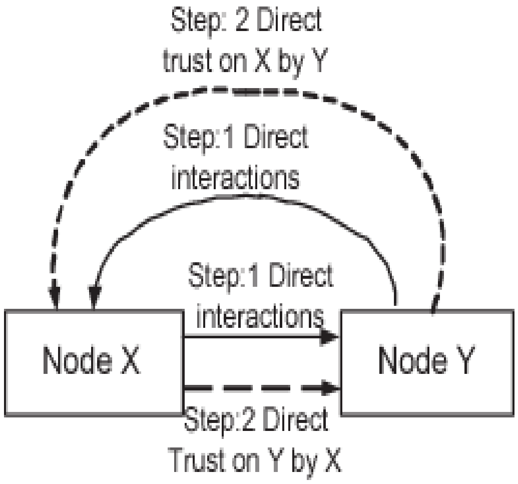
Step: 2 Direct trust on X by Y
Step:1 Direct interactions
Step:1 Direct interactions
Node X
Node Y
Step:2 Direct Trust on Y by X

Figure 3: Direct Trust Method

Indirect Trust: The indirect trust of any node on any neighbouring node can be evaluated from the indirect information given by the neighbouring nodes. Again, as in trust metrics, the neighbouring nodes are also divided into the most trusted and normal other neighbouring nodes. The geometric mean will be calculated to the data given by the most believed neighbouring hubs and also the arithmetic means will be calculated to the data given by the other ordinary neighbouring hubs. A chance can be given to expect for the computation of IT the arrangement of hubs (state 8) that are arranged in some adjacent region in the WSN field which has appeared in Figure 4.Their names are A, B, C, D, E, F, G, H, and I. Here, we are interested to find the IT of node A on the neighbouring node B. The node A first collects the recommendations from their neighbouring nodes. In this case, nodes C, D, E, F, G, H and I are neighbours.

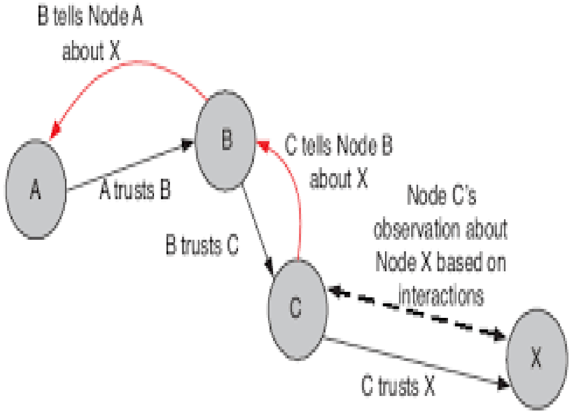

Figure 4: Indirect Trust Method

Analytic Network Process: The proposed model calculates the trust value of the node based on the ANP [12]. Measuring the trust value of a node is always a challenging problem [13, 14]. A node's trustworthiness is often related to the quality of services it provides to others. If the quality of service will be objectively measured, then associate degree entity's trustiness for that service is termed objective trust. The trusted path obtained by using the ANP decision theorem eliminates the malicious nodes and helps to protect the network from any internal attacks.

The trust model of an ad-hoc network can be represented as the weighted directed graph as in the Fig.3. Each node in the model maintains a trust table which contains the trust values of the neighbouring nodes.

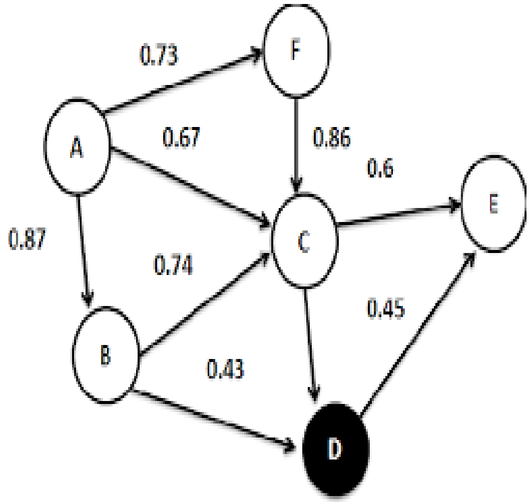

Figure 5: Selection of a trusted node

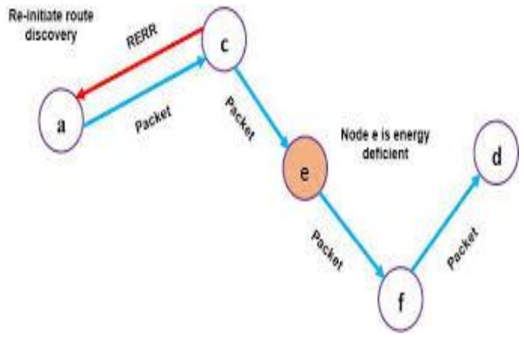

Figure 6: Neighbouring nodes periodically exchange Hello Message

VI. TOOLS AVAILABLE IN NETWORKINGFIELD

Table 1. Simulation tools used in finding the trusted node in Networking

S.No	Simulation tools	Description
1	NS3	The main focus is on wireless/IP simulations which involve models for layers 1 and 2 with a variety of static or dynamic routing protocols such as OLSR and AODV for IP-based applications.
2	NS2	It is used to model the behavior of the simulation nodes, and OTcl scripts that handle the simulation and specify the network topology
3	OMNet++	OMNeT++ is an eclipse based IDE graphical runtime environment.
4	NetSim	It supports major technologies like wireless (LAN, Wi-Max, MANET, WSN, Wi-Fi), MPLS, QoS, VoIP, TCP, IP, etc.
5	OPNET	It provides simulation, analysis, and design of networks, applications (terrain modeling, system-in-the-loop, 3D network visualizer, app transaction expert models application transactions)
6	REAL	The GUI allows users to quickly build simulation scenarios with drag and draw interfaces
7	J-Sim	J-Sim is in Java language. It supports scripting with Perl, Tcl, or Python interface for integration

VII. CONCLUSION

In this paper, a traditional trust management models and Analytic Network process models have been studied to select the trusted nodes which exclude the malicious nodes in order to establish secure communication. The trust Model factors are obtained and they include Direct Trust, Indirect trust, and Analytic Network Process. Based on the trust decision factors, the selection of the trusted nodes is obtained by using the Analytic Network Process (ANP). It reduces a multidimensional problem into a one dimensional one. Decisions are determined by a single number for the best outcome or by a vector of priorities that gives an ordering of the different possible outcomes. The trust model ANP can kick out the untrustworthy nodes and selects only the trustworthy nodes in the network so that a reliable passage delivery route is obtained. Hence we planned to adopt Analytic Network process methodology in our research work. To make a further improvement for the trust prediction model discussed in this paper, we plan to incorporate other decision factors to our trust model. The problem of vibrant behaviour modification will also be measured. In addition, a new trusted dynamic source routing protocol will be proposed.

REFERENCES

[1] R. Li, J. Li, P. Liu, and J. Kato, “A Novel Hybrid Trust Management Framework for MANETs,” in Proc. 29th IEEE Int. Conf. Distrib. Comput. Syst. Workshops, 2009, pp.251–256.

[2] J. Luo, X. Liu, and M. Fan, “A Trust Model Based on AFuzzy Recommendation for Mobile Ad-hoc Networks,” Comput. Netw., vol. 53, no. 14, pp. 2396–2407, 2009.

[3] Satty, T.L.: “The Analytic Hierarchy Process” (McGraw-Hill, New York, 1980).

[4] Xia, Hui, et al. "Trust Management Model for Mobile Ad hoc Network Based on Analytic Hierarchy Process and Fuzzy Theory." Wireless Sensor Systems, IET1.4 (2011): 248-266.

[5] Sun, Y. L., Yu, W., Han, Z., Ray, L. K. J.: “Trust Modeling and Evaluation in Adhoc Networks”.Proc. Global Telecommunications, 2005,pp.1–10.

[6] Sun, Y.L., Yu, W., Han, Z., Ray, L. K. J.: “Information Theoretic Framework of Trust Modeling and Evaluation for Ad hoc Networks”, IEEE J. Sel.Areas Commun., 2006, 24, (2), pp.305–319.

[7] Josang, A.: “A Logic for Uncertain Probabilities”, Int. J. Uncertainty, Fuzziness, Knowledge-Based Syst., 2001, 9,(3),pp 179–311 13.

[8] Beth, T., Borcherding, M., Klein, B.:“Valuation of Trust in Open Network”.Proc.ESORICS, 1994, pp.3–15.

[9] H.Yu, S. Liu, A.C.Kot, C.Miao, and C.Leung, ‘’Dynamic Witness Selection for Trustworthy distributed Cooperative Sensing in Cognitive Radio Networks’’, Communication Technology (ICCT), 2011 IEEE 13th International Conference on, pp. 1-6, 2011.

[10] P. B. Velloso, R. P. Laufer, D. de O Cunha, O.C.M.Duarte, and G.Pu-jolle, ‘’Trust Management in mobile ad hoc networks using a

scalable maturity-based model,’’Network and Service Management, IEEE Transactions on, 7, (3), pp. 172-185, 2010.

[11] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, “E-Hermes: A Robust Cooperative trust establishment scheme for mobile Ad-hoc Networks,” Ad Hoc Netw., vol. 7, no. 6,pp. 1156–1168, 2009.

[12] Saaty, Thomas L. "Analytic Network Process." Encyclopedia of Operations Research and Management Science.Springer US, 2001 8-35.

[13] Y. L. Sun, W. Yu, Z. Han, and K. Liu,” Information theoretic framework of trust modeling and evaluation for ad hoc networks, “IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, pp 305-317, Feb 2006.

[14] X. Li, M. R. Lyu, and J. Liu, “A trust model based routing protocol for secure ad hoc networks,” in Proceedings 2004 IEEE Aerospace Conference, Big Sky, Montana, U.S.A., March 6-13 2004.

[15] Xiao - Lin, LI Xiao - Yong GUI. "Trust Quantitative Model with Multiple Decision Factors in Trusted Network [J]." Chinese Journal of Computers 3 (2009): 004.

[16] Xia, Hui, et al."A Subjective Trust Management Model with Multiple Decision Factors for MANET Based on AHP and Fuzzy Logic Rules." Proceedings of the 2011 IEEE/ACM International Conference on Green Computing and Communications. IEEE Computer Society, 2011.

[17] Lubdha M. Bendale, Roshani. L. Jain, Gayatri D. Patil, "Study of Various Routing Protocols in Mobile Ad-Hoc Networks", International Journal of Scientific Research in Network Security and Communication, Vol.06, Issue.01, pp.1-5, 2018.

[18] Afzal Ahmad, Mohammad Asif, Shaikh Rohan Ali, "Review Paper on Shallow Learning and Deep Learning Methods for Network security", International Journal of Scientific Research in Computer Science and Engineering, Vol.6, Issue.5, pp.45-54, 2018.

AUTHOR’S PROFILE

G.Viswanathan pursued Bachelor of Science from Madras University and Master of Science from Periyar University in 2001. He completed Master of Philosophy in Computer Science from Bharathidasan University in 2005. He is working as an Associate Professor in Department of Computer Technology in SNMV College of Arts & Science, Coimbatore. His Area of Interest is Computer Networks. He has guided for 11 M.Phil students. He is lifetime member of ISTE. He has 17 year of teaching experience at UG and PG level.

Dr.M.Jayakumar pursued Doctor of Philosophy in Computer Science at Government Arts college, Udumalpet, Affiliated to Bharathiar University in 2015. He is working as an assistant Professor in Department of Information Technology in SNMV College of Arts & Science, Coimbatore. His specialization is Network Security. He has 6 years of Teaching Experience and 7 years of Industry Experience.