International Journal of Engineering & Technology, *7 (2.21) (2018) 402-404*

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A study on reliability of Manets using trust management system

G. Bindu[1*], R.A. Karthika [2], S. Sridevi [3]

[1]Department of Computer Science and Engineering, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India.
[2]Department of Computer Science and Engineering, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India.
[3]Department of Computer Science and Engineering, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India.
**Corresponding author E-mail: bindu.se@velsuniv.ac.in*

Abstract

Mobile Adhoc Networks is a network where nodes keep moving geographically and doesn't have an infrastructure. This network is a challenging when interactions are critical to attain system goals like reliability, configurability, capability to increase the size of networks, rapid changes in topology of network, this effects the new nodes entering the network easily to attack. This makes difficult to maintain Trust management in the MANET. To overcome this, few algorithms are developed for Trust management. In this paper we discussed the different types of MANET, Applications, protocols and Trust management schemes. We tried to derive the trust management from different fields.

Keywords: *MANET (Mobile Adhoc Networks),Trust, protocols.*

1. Introduction

MANET is a type of network in which the nodes move geographically .As the nodes always in motion these networks use wireless connections .Each individual nodes is autonomous. This network may contain different mobile devices which are arranged in various topologies. MANETs can be arranges in many setups which is still being observed. The major challenge of MANET is detection of malicious nodes.

- Vehicular ad hoc networks (VANETs) in this network vehicles and other devices are connected using artificial intelligence to protect from accidents, vehicle to vehicle collisions.
- Smart phone ad hoc networks (SPANs) By using the existing hardware (Blue tooth and Wi-Fi) available in mobile phones to create peer-to-peer networks without traditional network infrastructure and wireless access point. A node can join at any time without disturbing network.
- Internet-based mobile ad-hoc networks In this network it supports UDP/TCP and IP internet protocols. It uses network layer protocol to connect mobile nodes to create routes automatically.
- Mobile ad hoc networks can be used in many applications such as environment, vehicular Adhoc communications, road safety, robots, air/land/navy defence, health, weapons.

The contribution of this paper is:

1. Discussing mobile Adhoc protocols and types.
2. Defining Trust in communication and networking field.
3. Survey of existing trust management schemes.

2. Routing protocols used in manet

An ad hoc routing protocol is a method how a packet route in a MANET between computing devices. The types of protocols are
Proactive: In this type of protocols Routing table is maintained for future reference. This is prone to failures OLSR, **D**SDV, DREAM etc are examples
Reactive: This does not find any routing table. It dynamically takes a decision to route a packet It consumes more time to identify the route. Also it increases the network traffic by flooding packets AODV, DSR etc are examples.
Hybrid: This combines the both features of Pro Active and Reactive Protocols Advantage depends on number of other nodes activated. ZRP (Zone Routing Protocol), ZHLS (Zone-based Hierarchical Link State Routing Protocol) etc. are examples.

3. Design challenges in Manet Protocols

A mobile Adhoc networks [1] consists of node connected through wireless sensor nodes (devices). These nodes communicate each other through multi hops for designing protocols for this type of network is a big challenge as there is a limitation of resources and band width.[1] [2] [3].
Developing security protocols for military Manet needs more caution as a military operation must support aggressive environment, different types of nodes often poor performance constraints leading to often changes in topology of networks and node may not have free defined trust relationship [4].
To over these difficulties a network should use a low complexity distributed network management schemes.

4. Possible attacks in manet

Eavesdropping – the intruder try to attack in physical layer to do eavesdropping.
Jamming - It always attacks flood servers. It increases traffic wantedly to bring. Attacks under the control of attackers
Block hole – in this attack the attacker mode acts in a way to divert the packet into its control by giving wrong routing direction. It acts as its having optimal path to route the path.
Worm hole - It is also called as tunnelling attack. Confidential information is transferred between two malicious nodes by acting as neighbours. In this type of attack multiple malicious nodes interact each other to intrude.
Gray hole - It is same as black hole attack but in this kind of attack attacker sometimes drops the packets and sometimes behaves like normal node.
Link spoofing - Attacker advertise as being two hop neighbour with fake links and manipulate data.
Rushing –when a route request is sent the intruder node try to act as a real source.
Flooding - Network is flooded with false routing information by malicious node and consumes network resources. It is also called as resource consumption attack.

5. Concept of trust management in Manets

Definition: The Term originates from social science and defined as degree of Belief depending upon behaviour of particular entity [5] [6]. Trust is the degree of belief in forwarding the data packets successfully without any attacks. Trust of each node in the network is unique. Trust is relationship between two entities so that the one expects beneficial reliable communication Trust management is considered as separate important component of a security services in networks. Trust in Manet is considered as an important property when two nodes are communicating with no previous interactions. In building initial trust bootstrapping [7], group of operations without predefined trust and authentication of certificates generated for ensuring security before entering a new zone [8]. Trust management is implemented in many decision making situations like intrusion detection, access control, and key management, identifying misbehaving nodes for effective routing.
A mobile Adhoc networks is always works is an environment where there is no fixed network topology therefore reduces the cost of deployment [12]. The method of "trust modelling" is a good way of approaching a specific element in networking practically. "Trust administration used for finding and translating security approaches [13], qualifications, and connections." Trust administration takes care of secure directing, key administration, verification, and access control and recognizing interruption .The quality of trusted nodes is more than untrusted nodes. The entire quality of node depends on social behaviour of individual nodes.

Trust Metrics

Trust can be measured in different ways using continuous, discrete or Boolean values. For example, Trust can be given values as [0, 1] or [-1, 1] or [F, T]. Trust metrics can be calculated using methods like Fuzzy, Probability, Similarity, Mobility, etc
Let us consider two nodes P and K communication the trust of P to K is T(K, P) and the trust of K to P is T(P, K) if K successfully forwards packet to Y then the value T(K, K) is increased ,Otherwise T(K, P) will be decreased.

Properties of Trust in MANETs

- A trust can never formed with a cooperative behaviour of a node for MANETs.
- Trust should be evaluated in an easy way.
- Trust is not static, it often change.
- Trust is subjective.
- Trust is not transitive in nature.
- Trust is not a reciprocal one.
- Trust is context based.

Trust phases

- Trust Establishment.
- Trust Updation.
- Trust Revocation.

6. Discussion of existing methods

For detection of malicious node in a network is a challenging task. This is achieved by so many ideas among them trust management system, one of the efficient method.

1. Probabilistic coverage algorithm

Zahra Taghikkaki, Nirvana Mehratnia [19] observing the coverage area of a wireless sensor network as the sensing resources are very less, the measurements associated with them are limited inherent. So, QOS based coverage scheme is needed. In this, author proposed a trust based probabilistic coverage algorithm which deals with uncertainty in the environment of nodes. This uses a programming problem called integer linear programming, which uses QOS aware scheme. Greedy heuristic algorithm also used.

2. CH selection algorithms in MWSN

Eid Rehman, Muhammad Sher,[20] In this paper clutter head selection algorithm is explained and implemented in this paper. The different attributes of notes are considered. The parameter or attributes are inclined waiting time, connectivity degree and distance between notes. The selection of head of clusters depending on weights of a node. The scheme proved for avoiding malicious nodes and also energy efficiency.

3. Objective function

S. VenkateshBabu and Dr.C. KeziSelvaVijila [18] The trust of nodes are calculated by using trust parameter shared between the nodes with the use of objective function, which defines the degree of trust basing on node forwarding behaviour. There are different ways, direct and indirect method of calculating trust. In direct method trust is calculated basing on the behaviour of neighbour node and in indirect method the nodes calculates the trust value by observing from its neighbour node. This paper outlines the various trust management mechanisms which operates in vibrant and ambiguous MANET environment.

4. Advanced Hybrid Intrusion Detection System (AHIDS)

Rupinder Singh Jatinder Singh [17] proposed Advanced Hybrid Intrusion Detection System (AHIDS) is an algorithm which is very advantageous for WSNs. In this method the sensor nodes generally don't consumes much energy. AHIDS identifies misbehaviour and misuse of a node using fuzzy and neural networks. Also feed forward neural networks with back propagation. Using feed forward neural networks are used to collect the results information from different sensor node .AHIDS uses LEACH PROTOCOL.

5. Multi parameter metrics method

Pradnya M. Nanaware and Dr. Sachin D. Babar [17] Various parameter are taken in account to separate between malicious modes and trusted modes of the network. The parameter include energy of mode, mode motion and energy consumption and finally given the trust value based on metrics or attributes.

6. Cluster based trust routing protocol

F. Ba o et al. [14] demonstrated trust management protocol for WSNs.

This paper taken multiple attributes of trust which is calculated by coo operation of different informal organisation to interact with trust of sensor hubs. He explains about heterogeneous nature of WSN which in turn used to interact with different type of sensor hubs. Finally attaining to get ground truth. The proposed protocol is cluster based. Authors have considered multidimensional trust traits determined by correspondence and informal organizations to assess the trust of a sensor hub. Using novel likelihood model, authors have portrayed a heterogeneous WSN involving an extensive number of sensor hubs with limitlessly diverse social and nature of administration practices with the goal to get "ground truth" hub status.

7. Fuzzy logic based routing protocol

V. Balan et al. [15] The author used technique like fuzzy logic technique node blocking mechanism so that these techniques help to defect blackhole attack, gray node attack and different attack. The whole system consist of three main stages fuzzy implementation, categorisation and family estimation.

8. X.509 and PGP

This paper explained about the importance of security policies and security credentials. It checks whether it is satisfying recommendation of trusted third party. It also helps to check security levels of X.509 and PGP which is very useful for strong network.

9. Markov chain trust protocol

B. J. Chang et al. [16] The vulnerability of Manet makes difficult to work with. Trust based techniques reduced attacks to some extent. In markov chain the previous reading of modes are noted and used further in this technology for each nop modes trust value is calculated

7. Conclusion

This paper on MANET was to provide perspective concepts of trust to every MANET network protocol designers, and to give new concepts and ideas to develop the trust metric to meet the goals of the targeted system. We suggest the future programmers by introducing the concepts of social and cognitive networks, to develop trust management schemes with desirable attributes like adaptation to environment dynamics, stability, reliability, and re configurability.

Trust is a multidimensional, a complex thing which is hard to make and a context dependent concept. In everyday life trust plays an important role in decision making. The MANET faces trust establishment problems from severe resource constraints, the open nature of the wireless medium, the complex dependence between the communication network, the social network, the social network and application network, and hence the complex dependency of any trust metric to feature, parameters and introduction.

References

[1] Corson S & Macker J, "Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", RFC 2501, (1999).

[2] Jubin J & Tornow J, "The DARPA Packet Radio Network Protocols", *Proc. IEEE*, Vol.75, No.1, (1987), pp.21-32.

[3] Tardiff AJ & Gowens JW, "ARL Advanced Tele communication and Information Distribution Research Program (ATIRP)", *Final Report*, (2001).

[4] Plesse T, Lecomte J, Adjih C, Badel M, Jacquet P, Laouiti A, Minet P, Muhlethaler P & Plakoo A, "OLSR Performance Measurementin a Military Mobile Ad Hoc Network", *24th Int'l Conf.on Distributed Computing Systems*, (2004), pp.704-709.

[5] Cook KS, *Trust in Society*, Russell Sage Foundation Series on Trust, New York. Vol.2, (2003).

[6] Blaze M, Feigenbaum J & Lacy J, "Decentralized Trust Management", *IEEE Symposium on Security and Privacy*, (1996), pp.164 - 173.

[7] Bobba RB, Eschenauer L, Gligor V & Arbaugh W, "Boots trapping Security Associations for Routing in Mobile Ad Hoc Networks", *IEEE GLOBECOM, San Francisco*, (2003), pp.1511-1515.

[8] Eschenauer L, Gligor VD & Baras J, "On Trust Establishment in Mobile Ad Hoc Networks", *10th Int'l Security Protocols Workshop*, vol. 2845, (2002), pp.47-66.

[9] Baras JS & Jiang T, "Managing Trust in Self-Organized MobileAdhoc Networks", *12th Annual Network and Distributed System Security Symposium Workshop*, (2005).

[10] Ruhomaa S & Kutvonen L, "Trust Management Survey", P. Herrmannet al. (Eds.), iTrust, Lecture Notes in Computer Science, (2005).

[11] Pradnya MN & Dr. Sachin DB, "Trust System Based Intrusion Detection", *Mobile Ad-hoc Network (MANET)*", (2012).

[12] Jeroen H, Ingrid M, Bart D & Piet D, "An Overview of Mobile Ad-Hoc Networks: Applications and Challenges", *Journal of Communication Network*, Vol.3, (2004), pp.60-66.

[13] Ing RC, Jia G, Fenye B & Jin HC, "Trust management in mobile ad hoc networks for bias minimization and application performance maximization", *Elsevier*, (2014).

[14] Bao F, Chen IR, Chang M, Cho JH, "Trust-based intrusion detection in wireless sensor networks", *IEEE Int'l Conf. on Communication*, (2011), pp. 1–6.

[15] Vishnu Balan E, Priyan MK, Gokulnath C & Usha Devi G , "Fuzzy Based Intrusion Detection Systems in MANET ", *Elsevier*, (2015).

[16] Chang BJ & Kuo SL, "Markov chain trust model for trust value analysis and key management in distributed multicast MANETs", *IEEE Trans. Veh. Technol.*, Vol.58, No.4, (2009), pp.1846–186.

[17] Singh R, Singh J & Singh R, "Fuzzy Based Advanced Hybrid Intrusion Detection System to Detect Malicious Nodes in Wireless Sensor Networks", *Wireless Communications and Mobile Computing*, (2017).

[18] Babu SV & Vijila CKS, "Survey report on MANETs trust management", *Advances in Natural and Applied Sciences*, Vol.11, No.3, (2017), pp.138-146.

[19] Taghikhaki Z, Meratnia N & Havinga PJ, "A trust-based probabilistic coverage algorithm for wireless sensor networks", *Procedia computer science*, Vol.21, (2013), pp.455-464.

[20] Rehman E, Sher M, Naqvi SHA, Badar Khan K & Ullah K, "Energy Efficient Secure Trust Based Clustering Algorithm for Mobile Wireless Sensor Network", *Journal of Computer Networks and Communications*, 2017.