International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 9 Issue 9, September-2020, Impact Factor: 6.754

Trust-Based Scheme for Secure and QoS Routing in MANETs: A Survey

Janesh[1], Dr. Pawan Kumar[2], Dr. Sandeep Tayal[3], Dr. Deepak Goyal[4], Dr. Monika Goyal[5]

[1]M.Tech Scholor, Vaish College of Engineering, Department of ECE, Rohtak, Haryana, India Assistant
[2]Professor, Vaish College of Engineering, Department of ECE, Rohtak, Haryana,India
[3]Professor, Vaish College of Engineering, Department of ECE, Rohtak, Haryana, India
[4]Professor, Vaish College of Engineering, Department of CSE, Rohtak, Haryana, India
[5]Assistant Professor, Vaish Mahila Mahavidyalaya, Rohtak, Haryana, India

ABSTRACT

The advent of mobile ad hoc (MANET) network had spurred in a new era of communication where users (nodes) communicate with each other via a self configuring infrastructure less network of mobile devices connected by wireless links. The security is very vital aspect for implementing MANETs in adverse environment. Compared to wired networks, MANETS are more vulnerable to security attacks due to lack of a trusted centralized authority and easy eavesdropping. MANET is a self configuring network. Due to dynamic nature of MANET it is very challenging work to employ a secure route. Wireless medium as medium for communication and lack of centralized control renders MANETs a favorable victim of hackers and intruders. Other features like change in the topology due to node's movements, battery depletion at nodes and coverage hampering due to obstacles in random terrains etc. adds to miseries of Ad hoc networks. Various techniques based on cryptography, hash functions and trust etc have been developed.

Keywords: Routing Protocol, Wireless Sensor Network, Trust, Quality of Service, MANET, Security

1. INTRODUCTION

MANET

MANET is a self-configuring system of mobile routers linked by wireless links which consequently combine to form an arbitrary topology. The mobility of the routers are provided randomly and organized themselves arbitrarily. MANET has various potential applications, such as emergency search-rescue operations, meeting events, conferences, and battlefield communication between moving vehicles and/or soldiers [1]. MANET is a highly flexible network where nodes can freely move and join, with no fixed infrastructure, and thus it is vulnerable to attacks by malicious users. These types of attacks are basically unfeasible to detect, thus making it hard to produce security for such attacks [2].

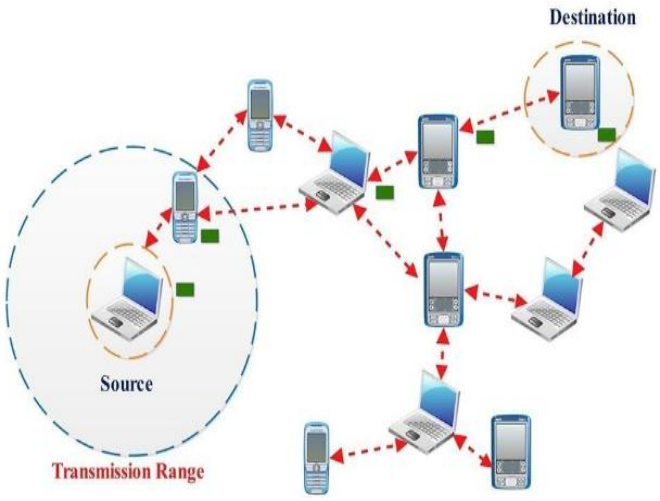

Figure 1 Architecture of MANET

Certificate system in MANET

A large number of methods to detect various kinds of attacks have been developed for MANETs. Only detecting and blocking attacks in each node is not enough to maintain network security because attackers can freely move and repeatedly launch attacks against different nodes. To reduce the damage from attacks, attackers must be immediately removed from the network after detection of the first attack; this can be achieved by using a certification system. In networks with the utilization of a certification system, nodes cannot communicate with each other without a valid certification. In other words, any attacker cannot exist in the network once its malicious behavior has been detected by others and its certification has been revoked accordingly by the system. The performance of a certification system largely depends on its deployed certification revocation strategy [3].

Issues

- Inaccuracy
- Slow revocation
- Network overhead [2]

Certificate distribution &revocation in MANET

They are based on the determination of the trustworthiness of nodes, regarding their recommended functionality. The prime goal of rational nodes is to cooperate in order to avoid, or even mutually isolate, notorious nodes (i.e., selfish, malicious) from routine network operations. Such cooperation requires the exchange of recommendations and the identification of trusted recommenders [11]. The system which is identifying the attackers based on the information on the occurrence of attacks provided by nodes belonging to the network, the certificate of a legitimate user might be revoked by the false accusation from malicious nodes. Therefore, certificate revocation methods must be able to distinguish false accusations from valid ones. Also, malicious nodes must be immediately removed from accessing the network with a small operating overhead [4].

2. ROUTING IN MANET

Routing Schemes in MANETs are classified into Reactive, Proactive and Hybrid category on the basis of mode of operation. Further classification is due to network structure and classes identified are Flat, Hierarchical and Location or Geography based routing schemes. Another Classification is due to Routing strategy and schemes in this class can be studied under QoS based and Multipath Routing schemes. Figure 2, presents a classification of routing protocols in MANETs [3].

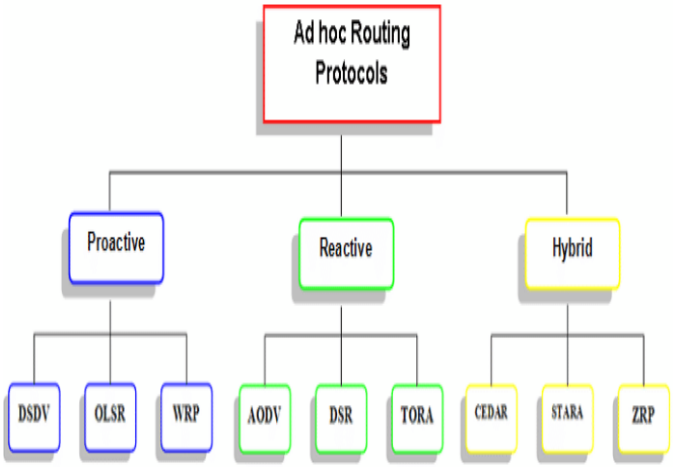

Figure 2 Routing protocol of MANET

Proactive Routing Protocols

Proactive class of routing schemes stores the routing information gathered from neighbouring nodes through periodic or event based updates. Information received via updates is maintained as routing tables. The change in the topology due to node movement, energy drain or physical obstacles or physical security attacks initiate next round of updates. Each node may maintain partial or total network topology and thus time and energy spent in convergence of routing information in nodes consume a lot of time and energy. There are times when nodes in the network may possess unstable routing information.

Reactive Routing Protocols

Proactive routing schemes suffer performance limitation due to frequent route updates due dynamic topology changes. To overcome these limitations and frequent topology changes, routes may be computed only when it is actually required. Reactive routing schemes follow the suit of temporal update and prevent the instances of unstable network state. DSR (Dynamic Source Routing), AODV (Ad hoc on demand Distance Vector) and TORA (Temporary Ordered Routing Protocol) [6] etc. are the representative routing schemes in this category.

Hybrid Routing Protocols

Often single feature routing protocols suffers from limitation due to its very mode of operations. Combining the best of two or more classes of protocols often covers the limitation of other class. Hybrid routing protocols combines the features of both reactive and proactive routing protocols and attempt to overcome the limitations of each class of protocols through some customizations in basic operation modes of constituting members. ZRP (Zone Routing Protocol), SHARP (Sharp Hybrid Adaptive Routing Protocol, DHAR (Dual-Hybrid Adaptive Routing) & ADV (Adaptive Distance Vector Routing), TORA etc. are the representative proposal in this categories.
UWSNs

3. TRSUT AND REPUTATION MECHANISM

Trust mechanism is introduced in the protocols to provide security in MANET. Trust is a value that is calculated on the basis of nodes action when needed. Trust is introduced to prevent from various attacks like wormhole, black-hole, Dos, selfish attack etc. Trust can be implemented in various ways such as by reputation, subjective logic, from opinion of nodes etc as there are no particular definitions of trust [11-13]. According to researchers trust has following properties:

Context Dependence: In some specific context trust relationships are applicable.

Function of uncertainty: Trust depends on the uncertainty of nodes action. It gives the probability of action performed by a node.

Quantitative value: Trust can be assigned any type of numeric values discrete or continuous.

Asymmetric Relationship: Trust relationship is asymmetric in nature. If node A trusts B and node B trust C that does not mean that A trusts C.

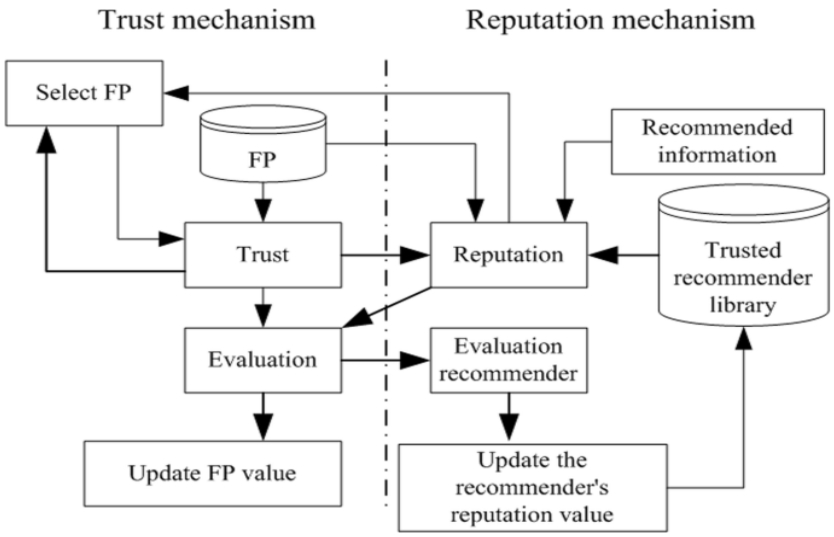

Figure 3 Trust and Reputation Mechanism

4. TYPES OF ATTACKS IN MANET

Objective: Due to these reasons the networks are more susceptible to different types of attacks. In MANETs, the attacks are broadly divided into two categories*; Passive* attacks and *Active* attacks [10]. The passive attacks typically involve eavesdropping of data only. Such attacks are hard to trace. Whereas the active attacks involve actions performed by the adversaries like:

Modification based attacks: Integrity of the packets is basically tampered with Modification attacks. With these attacks, the malicious nodes modify the contents of the packets while forwarding them to achieve a desired outcome.

Fabrication based attacks: When the malicious nodes generate and propagate the false routing messages in the network.

Impersonation based attacks: The Malicious nodes can initiate attacks by masquerading as genuine node, which is also known as spoofing. When a malicious node acquires the identity of genuine by varying its MAC or IP address with the mala-fide intention of cheat other nodes in the network. Some of the commonly known attacks in MANETs are Black hole Attack, Wormhole Attack, Rushing Attack, Jellyfish Attack, Sybil Attack, Byzantine Attack, Routing Table Overflow, Sleep Deprivation, and Denial of Service

Table 1 Layer based issues and attacks

Layer	Issues	Attacks
Physical Layer	Signal jamming, denial of service	DoS attack, Jamming, interceptions, eavesdropping.
Data Link Layer	Protecting the wireless MAC protocol and providing data link layer security support.	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness.
Network Layer	Protection of ad hoc routing and forwarding protocols.	Wormhole, Blackhole, Replay Routing, table overflow attacks.
Transport Layer	Authentication and securing end-to-end communication via encryption/de-encryption techniques	Session hijacking, flooding attack (SYN or ACK)
Application Layer	Detecting and preventing viruses, worms, and application abuses	Un-authorized access, Repudiation, data corruption

CONCLUSION

In summary, MANETs are vulnerable to different types of attacks due to its infra-structure less network. Different trust based approaches are proposed to prevent such types of attacks and to improve Quality of Services (QoS). These trust based approaches try to give a secure node in routing path by implementing trust mechanism in the existing routing protocols. In this paper, firstly we have given a brief idea on several types of attacks that MANET suffers and trust mechanism. Then we review currently existing trust based protocols and finally we have carried out a comparative study on these protocols on the basis of their merits and demerits.

REFERENCES

[1]. Navpreet Kaur, Manvinder Sharma, "Brain Tumor Detection using Self-Adaptive K-Means Clustering", International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS-2017)
[2]. Ms. Priya Patil, Ms. Seema Pawar, Ms. Sunayna Patil, Prof. Arjun Nichal, "A Review Paper on Brain Tumor Segmentation and Detection", International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, Vol. 5, Issue 1, January 2017
[3]. Uma-e-Hani, Saeeda Naz, Ibrahim A Hameed, "Automated Techniques for Brain Tumor Segmentation and Detection: A Review Study", Conference: 2017 International Conference on Behavioural, Economic, Socio- cultural Computing (BESC), DOI: 10.1109/BESC.2017.8256397
[4]. Ka Hei Loka, Lin Shib,c, Xianlun Zhud and Defeng Wanga, "Fast and robust brain tumor segmentation1 using level set method with multiple image information", Journal of X-Ray Science and Technology, DOI 10.3233/XST-17261, IOS Press

[5]. Reema Mathew A, Achala Prasad, Dr. Babu Anto P, "A Review on Feature Extraction Techniques for Tumor Detection and Classification from Brain MRI", 2017 International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT)
[6]. Hapsari Peni Agustin Tjahyaningtijas, "Brain Tumor Image Segmentation in MRI Image", Materials Science and Engineering 336 (2018) 012012 doi:10.1088/1757-899X/336/1/012012, IOP Publishing
[7]. Sanjay M. Shelke1, Dr. Sharad W. Mohod, "A Survey on Automated Brain Tumor Detection and Segmentation from MRI", International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 04 | Apr-201
[8]. S. Josephine, "Brain Tumor MRI Image Detection and Segmentation Using Genetic Algorithm", International Journal of Computer Sciences and Engineering, Volume-6, Special Issue-2, March 2018
[9]. Jide J. Popoola, Thompson E. Godson, Yekeen O. Olasoji, and Michael R. Adu, "Study on Capabilities of Different Segmentation Algorithms in Detecting and Reducing Brain Tumor Size in Magnetic Resonance Imaging for Effective Telemedicine Services", EJERS, European Journal of Engineering Research and Science Vol. 4, No. 2, February 2019