International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 07
June 2019

Review of Routing in MANET

Sonia Tyagi , Rakesh Chawla
[1]Department of Computer Science & Engineering
Delhi Institute of Technology and Management,
Deenbandhu Chhotu Ram University of Science & Technology (DCRUST), Sonepat
soniyatyagi1896@gmail.com
[2]Department of Computer Science & Engineering
Delhi Institute of Technology and Management,
Deenbandhu Chhotu Ram University of Science & Technology (DCRUST), Sonepat
rakeshchawla11@yahoo.com

Abstract— A Mobile ad hoc network is a collection of nodes where each node transfer (forward) packets to each other for communication. The communication can be inside the range or outside the range of transmission area. MANET requires neither require any centre administrator nor it requires fixed network infrastructure such as base stations for communication. It is a group of autonomous mobile users that interact with each other through wireless link. The topology of ad hoc networks is not fixed and not changes over time as the nodes moves from one location to another. In this paper we provide review of different Mobile Ad hoc Networks.

Keywords— Adhoc Networks, MANETs, VANETs

I. Introduction

Mobile Ad-hoc network is a set of wireless devices called wireless nodes, which dynamically connects and transfer information. Wireless nodes can be personal computers (desktops/laptops) with wireless LAN cards, Personal Digital Assistants (PDA), or other types of wireless or mobile communication devices. The figure below shows the basic concept of Mobile Ad hoc Network. Figure shows different wireless nodes (computing devices) for transferring data and information using air as the transmission medium. These wireless nodes provide wireless communication between different sources and destinations such as vehicle, plane or person.

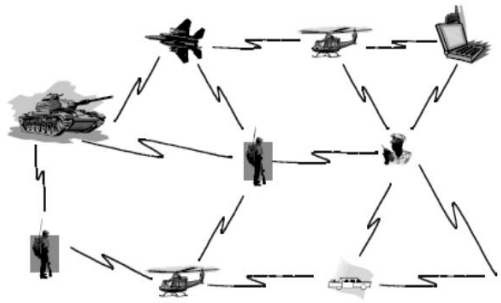

Figure : Mobile Ad-hoc Network In MANET

In MANET, a wireless node can be the source, the destination, or an intermediate node of data transmission. When a wireless node plays the role of intermediate node, it serves as a router that can receive and forward data packets to its neighbor closer to the destination node. due to the nature of an ad-hoc network, wireless nodes tend to keep moving rather than stay still. Therefore the topology of ad hoc networks is not fixed and not changes over time.

MANET provides following benefits to its users:

i) Low cost of deployment: Ad hoc networks can be deployed on the fly; hence no expensive infrastructure such as copper wires or data cables is required.

ii) Fast deployment: Ad hoc networks are very convenient and easy to deploy since there are no cables involved. Therefore Deployment time of ad hoc networks take less time.

iii) Dynamic Configuration: Ad hoc network configuration can change dynamically over time. We can easily change/modify the topology of Ad hoc network as compare to Local Area Network configuration.

MANET has various potential applications. Some typical examples include emergency search-rescue operations, meeting events, conferences, and battlefield communication between moving vehicles and/or soldiers. From the above applications we can conclude that MANET becomes the essential part of mobile computation.

In this paper we provide review of different Mobile Ad hoc Networks. We also provide propose system for trust based routing in MANET so that packets transfer from source to destination correctly & timely.

II. Characteristics of MANET

Mobile ad hoc network nodes are furnished with wireless transmitters and receivers using antennas, which may be highly directional (point-to-point), Omni-directional (broadcast), probably steerable, or some combination there. At a given point in time, depending on positions of nodes, their transmitter and receiver coverage patterns, communication power levels and co-channel interference levels, a wireless connectivity in the form of a random, multi-hop graph or "ad hoc" network exists among the nodes. As node moves the ad hoc topology also modifies to maintain transmission and reception.

We can summarize the characteristics of MANET as follows:

i. To perform communication without wire.
ii. Nodes can perform the rolls of both hosts and routers.
iii. There is constraint on Bandwidth and capacity links are not fixed.
iv. To perform operation which are Energy-constrained?
v. Limited Physical Security.
vi. To modify network topology as nodes move.
vii. To update the route as needed.

III. Literature Review

Different papers provide different types of research work for Mobile Ad Hoc Networks which are explained below.

Marti et al. [1] proposed a reputation-based trust management scheme that consists of a watchdog that monitors node behaviors and a path rater that collects reputation and takes response actions (e.g., isolating misbehaving nodes as a result of misbehavior detection). This work is an initiative to dynamically incorporate direct observations into trust values for secure routing. It extends DSR (Dynamic Source Routing) but trust evaluation is based only on direct observations. put in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so. To mitigate this problem, we propose categorizing nodes based upon their dynamically measured behavior. We use a watchdog that identifies misbehaving nodes and a pathrater that helps routing protocols avoids these nodes. Through simulation we evaluate watchdog and pathrater using packet throughput, percentage of overhead (routing) transmissions, and the accuracy of misbehaving node detection. When used together in a network with moderate mobility, the two techniques increase throughput by 17% in the presence of 40% misbehaving nodes, while increasing the percentage of overhead transmissions from the standard routing protocol's 9% to 17%. During extreme mobility, watchdog and pathrater can increase network throughput by 27%.

P Narayan [2], introduced a modified design of trust based dynamic source routing protocol to improve the quality. Each node would evaluate its own trusted parameters about neighbors through evaluation of experience, knowledge and recommendations. This protocol discovers multiple loop-free paths which are evaluated by hop count and trust. This judgment provides a flexible and feasible approach to choose a shortest path in all trusted path. The proposed protocol reduces the packet loss due to malicious nodes to a considerable extent thereby enhancing the performance. The author also compares the simulation results of with and without the proposed secure trust based model. The simulation results demonstrate that the PDR for STBDSR falls from 92% to 80%. A mobile ad-hoc network is a self-configuring network of mobile hosts connected by wireless links which together form an arbitrary topology. Due to lack of centralized control, dynamic network topology and multihop communications, the provision of making routing secure in mobile ad hoc networks is much more challenging than the security

in infrastructure based networks. But due to their limitations, there is a need to make them robust and more secure so that they can go well with the demanding requirements of ad hoc networks.

Theodorakopoulos and Baras [4] analyze the issue of evaluating the trust level as a generalization of the shortest-path problem in an oriented graph, where the edges correspond to the opinion that a node has about other node. They consider that nodes use just their own information to establish their opinions. The opinion of each node includes the trust level and its precision. The main goal is to enable nodes to indirectly build trust relationships using exclusively monitored information. Several protocols have been developed to secure Ad-hoc networks using cryptographic schemes, but all dependent on the existence of central trust authority. The presence of central trust authority is an impractical requirement for Ad-hoc networks, so in this Paper we present a trust model that doesn't rely on central trust authority. n our model we make use of trust agents that reside n etwork nodes. Each agent operates independently and maintains its individual trust value. An agent gathers data from all events & assigns weights to each event and computes different trust levels based upon them. Each trust agent basically performs the three functions: Trust Derivation, Quantification, and Computation.

Sun et al. [5] proposed trust modeling and evaluation methods for secure ad hoc routing and malicious node detection. The unique part of their design is to consider trust as a measure of uncertainty that can be calculated using entropy. In their definition, trust is a continuous variable, and does not need to be transitive, thus capturing some of the characteristics of trust in MANETs. However, this work considers packet dropping as the only component of direct observations to evaluate trust. In the proposed framework, trust is a measure of uncertainty with its value represented by entropy. We develop four Axioms that address the basic understanding of trust and the rules for trust propagation. Based on these axioms, we present two trust models: entropy-based model and probability-based model, which satisfy all the axioms. Techniques of trust establishment and trust update are presented to obtain trust values from observation. The proposed trust evaluation method and trust models are employed in ad hoc networks for secure ad hoc routing and malicious node detection. A distributed scheme is designed to acquire, maintain, and update trust records associated with the behaviors of nodes' forwarding packets and the behaviors of making recommendations about other nodes.

Balakrishnnan et al. [6] developed a trust model to strengthen the security of MANETs and to deal with the issues associated with recommendations. Their model utilizes only trusted routes for communication, and isolates malicious nodes based on the evidence obtained from direct interactions and recommendations. Their protocol is described as robust to the recommender's bias, honest-elicitation, and free-riding. This work uniquely considered a context-dependency characteristic of trust in extending DSR. In these models, recommendations are circulated by forwarding explicit messages or introducing extra message headers. Apart from incurring additional overhead, the recommendations are prone to issues such as recommender's bias, honest-elicitation, and free-riding. In this paper, we propose a trust model to enhance the security of mobile ad hoc networks and to address the issues related to recommendations. The model uses only trusted routes for communication, and isolates malicious nodes depending on the evidence collected from direct interactions and recommendations. It deploys a novel approach for communicating recommendations such that they are free from recommender's bias, honest elicitation, and free-iding. Simulation results confirm the effectiveness of our model.

Moe et al. [7] proposed a trust-based routing protocol as an extension of DSR based on an incentive mechanism that enforces cooperation among nodes and reduces the benefits that selfish nodes can enjoy (e.g., saving resources by selectively dropping packets). This work is unique in that they used a hidden Markov model (HMM) to quantitatively measure the trustworthiness of nodes. In this work, selfish nodes are benign and selectively drop packets. Performance characteristics of the protocol when malicious nodes perform active attacks such as packet modifications, identity attacks, etc., need to be investigated further.

K. Selvavinayaki [8] presents a survey of trust based secure routing protocols for mobile ad hoc networks. Different trust based secure routing protocols are discussed and analyzed in the paper along with their strengths, weaknesses and future enhancements. The routing attack addressed in this paper is the black hole attack. The Black hole attack is that where a malicious node advertises itself as it is having the optimal route to the destination. Most of the Routing

protocols do not address the issues of the routing attack. This paper describes a solution strategy which will overcome the black hole attacks in MANETs. The proposed solution is that the nodes authenticate each other by issuing security certificate in digital form to all the other nodes in the network. The proposed method is to be adapted on DSR protocol .This method is capable of detecting and removing black hole nodes in the MANET.

IV. Applications of MANET

Mobile ad hoc networks have been employed in scenarios where an infrastructure is unavailable, the cost to deploy a wired networking is not worth it, or there is no time to set up a fixed infrastructure. In all these cases, there is often a need for collaborative computing and communication among the mobile users who typically work fire fighters facing a hazardous emergency, policemen conducting surveillance of suspects, and soldiers engaging in a fight. When we consider all these usual driving applications managed by specialized people, we understand why there is a slow progress in deploying commercial ad hoc applications to ordinary people. This situation may change with the deployment of opportunistic ad hoc networks. These networks aim to enable user communication in an environment where disconnection and reconnection are common activities and link performance is dynamic. They are very suitable to support the situation where a network infrastructure has limited coverage and users have "islands of connectivity."

By taking advantage of device mobility, information can be stored and forwarded over a wireless link when a connection "opportunity" arises, such as an appropriate network contact happens. In this view, the traditional MANET incorporates the special feature of connection opportunity. A MANET can be used to provide access to crisis management applications, such as in a disaster recovery, where the entire communication infrastructure is destroyed and establishing communication quickly is crucial. By using a mobile ad hoc network, an infrastructure could be set up in hours rather than days or weeks, as in the case of a wired networking. One of many possible uses of a mobile ad hoc network is in noncritical and collaborative applications.

One example is a business environment where the need for collaborative computing might be more important outside the office, such as in a business meeting at the client's office to discuss a project. Another viable example is to use a mobile ad hoc network for a radio dispatch system. This system can be used, for instance, in a taxi dispatch system based on MANET. When a user wants to use an existing application on the Internet in a mobile ad hoc network, it is important to investigate its performance. This is the case, for instance, of Gnutella, one of the most widely used peer-to-peer systems, which needs to be evaluated before putting it through typical ad hoc conditions such as node mobility and frequent network partitioning.
Another application area is communication and coordination in a battlefield using autonomous networking and computing. Some military ad hoc network applications require unmanned, robotic components. Unmanned Airborne Vehicles (UAVs) can cooperate in maintaining a large ground mobile ad hoc network interconnected in spite of physical obstacles, propagation channel irregularities, and enemy jamming. The UAVs can help meet tight performance constraints on demand by proper positioning and antenna beaming. A vehicular ad hoc network (VA NET) is a mobile ad hoc network designed to provide communications among close vehicles and between vehicles and nearby fixed equipment.

V. Conclusion

Mobile Ad-hoc network is a set of wireless devices called wireless nodes, which dynamically connects and transfer information. Wireless nodes can be personal computers (desktops/laptops) with wireless LAN cards, Personal Digital Assistants (PDA), or other types of wireless or mobile communication devices. A Mobile ad hoc network (MANET) is a collection of nodes where each node transfer (forward) packets to each other for communication. The communication can be inside the range or outside the range of transmission area. In this paper we provided review of different Mobile Ad hoc Networks.

References

[1]. S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. 6th Annual ACM/IEEE Mobile Computing and Networking, Boston, MA, Aug. 2000, pp.255- 265.

[2]. P Narayan, V R. Syrotiuk, "Evaluation of the AODV and DSR Routing Protocols Using the

MERIT Tool", In proceeding or ADHOC-NOW 2004, pp25-36

[3]. Sun, Y., Yu, W. ,Han, Z.,and Liu, K.J.R.:'Information Theoretic Framework of Trust Modeling and Evaluation for AdHoc Networks', IEEE Journal on Selected Areas in Communications, 2006, 24, (2),pp. 305-317

[4]. G. Theodorakopoulos and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks," IEEE J. Sel. Areas Commun., Volume 24-no. 2, Feb. 2006.

[5]. Y. L. Sun, W. Yu, Z. Han, and K. J. R. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," IEEE J. Sel. Areas Commun., vol. 24, no. 2, Feb. 2006, pp. 305-317.

[6]. V. Balakrishnnan, V. Varadharajan, U. K. Tupakula, and P. Lucs, "Trust and Recommendations in Mobile Ad Hoc Networks," Int'l Conf. on Networking and Services, Athens, Greece, 19-25 June 2007, pp. 64-69.

[7]. M. E. G. Moe, B. E. Helvik, and S. J. Knapskog, "TSR: Trust-based Secure MANET Routing using HMMs," Proc. 4th ACM Symposium on QoS and Security for Wireless and Mobile Networks, Vancouver, British Columbia, Canada, 27-28 Oct. 2008, pp. 83-90.

[8]. K.Selvavinayaki, K.K.Shyam Shankar, Dr.E.Karthikeyan "Security Enhanced DSR Protocol to Prevent Black Hole Attacks in MANETs" International Journal of Computer Applications (0975 – 8887) Volume 7– No.11, October 2010

[9]. Li, Xin; Jia, Zhiping; Wang, Haiyang;"Trust-based On-demand Multipath Routing in Mobile Ad Hoc Networks" IET Information Security.

[10]. J. Sen, P. Chowdhury, and I. Sengupta, "A Distributed Trust Mechanism for Mobile Ad Hoc Networks," Int'l Symposium on Ad Hoc and Ubiquitous Computing, 20-23 Dec. 2006. Surathkal, India, pp. 62-67.

[11]. S. Buchegger and J. Boudec, "Performance Analysis of the Confidant Protocol," Proc. Int'l Symp. Mobile Ad Hoc Networking and Computing, 2002.

[12]. M. Guerrero Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," Proc. ACM Workshop on Wireless Security (WiSe), ACM Press, 2002, pp. 1–10.

[13]. K. Sanzgiri et al., "A Secure Routing Protocol for Ad Hoc Networks," Proc. 10th IEEE Int'l Conf. Network Protocols (ICNP '02), IEEE Press, 2002, pp. 78–87.

[14]. P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," Proc. IFIP TC6/TC11 Sixth Joint Working Conf. Comm.and Multimedia Security, 2002.

[15]. Yi, S., Naldurg, P., Kravets, R., "Security aware ad-hoc routing for wireless networks," Proc. of the 2nd ACM International Symposium on Mobile ad hoc networking and computing (MobiHoc'01), 2001, pp. 299-302.