Selfish Attack Detection in Mobile Ad hoc Networks

A seminar report
submitted in partial fulfillment of
the requirements for the award of the degree of
BACHELOR OF TECHNOLOGY

in

Department of Computer Science And Engineering

from

University Of Calicut

Submitted By

SAJIHE C. K. (CEAOECS066)

MEA ENGINEERING COLLEGE
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
VENGOOR P.O, PERINTHALMANNA, MALAPPURAM, KERALA-679325
APRIL 2018

MEA ENGINEERING COLLEGE

PERINTHALMANNA-679325

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

*This is to certify that the seminar report entitled "***Selfish Attack Detection in Mobile Ad hoc Networks***" is a bonafide record of the work done by* **SAJIHE C. K. (CEAOECS066)** *under our supervision and guidance. The report has been submitted in partial fulfilment of the requirement for award of the Degree of* **Bachelor of Technology** *in* **Department of Computer Science And Engineering** *from the University of Calicut for the year 2018.*

Dr. Abdul Gafur M.
Head Of Department
Dept.of Computer Science and Engineering
MEA Engineering College

Mr. Anish Kumar B.
Seminar Guide
Assistant Professor
Dept.of Computer Science & Engineering
MEA Engineering College

ACKNOWLEDGEMENT

An endeavor over a long period may be successful only with advice and guidance of many well wishers. I take this opportunity to express my gratitude to all who encouraged me to complete this seminar. I would like to express our deep sense of gratitude to my resepcted **Principal Dr. Rajin M. Linus** for his inspiration and for creating an atmosphere in the college to do the project.

I would like to thank **Dr. Abdul Gafur M. , Head of the department, Computer Science and Engineering** for providing permission and facilities to conduct the seminar in a systematic way. I am highly indebted and thankful to **Mr. Anish Kumar B., Asst. Professor in Computer Science and Engineering** for guiding me and giving timely advices, suggestions and whole hearted moral support in the succesful completion of this seminar.

My sincere thanks to seminar co-ordinator **Mr. Muhammed Saleem P., Asst. Professor in Computer Science and Engineering** for his wholehearted moral support in completion of this seminar.

Last but not least, I would like to thank all the teaching and non-teaching staff and my friends who have helped us in every possible way in the completion of my seminar.

DATE:14-04-2018 SAJIHE C. K. (CEAOECS066)

ABSTRACT

Combine effort of nodes in Mobile Ad hoc Network makes it more powerful. But supporting a MANET is a costintensive activity for a mobile node. Route discovery and packets forwarding consumes bandwidth and energy. One such routing misbehavior of node is some nodes may be act as selfish by taking part in route discovery and maintenance process, but deny forwarding the packet. Such type of misbehavior reduce packet delivery ratio and also degrade system performance in terms of power and bandwidth. MANETs is lack in centralized monitoring and infrastructureless behavior makes it more vulnerable to attack, and difficult to detect selfish node effectively. This paper surveys existing latest developments in selfish attack detection system in MANETs. Based on existing study drawbacks, we have proposed assignment based Social Selfishness detection technique in mobile ad hoc networks. Finally, we conclude this some future work as a simulation in network simulator 2.

Contents

CHAPTER 1

INTRODUCTION

Mobile Wireless Ad hoc Network (MANET) is a group of autonomous mobile nodes or devices connected through wireless links without the support of a communications infrastructure. The topology of the network changes dynamically as nodes move and the nodes reorganize themselves to enable communications with nodes beyond their immediate wireless communications range by relaying messages for one another , i.e. multihop. MANET relies on the cooperation of all the participating nodes.

The more nodes cooperate to transfer traffic, the more powerful a MANET becomes. But supporting a MANET is a cost-intensive activity for a mobile node. Detecting routes and forwarding packets consumes networkbandwidth, local CPU time, memory, and energy.

Therefore there is a strong motivation for a node to deny packet forwarding to others, while at the same time using their services to deliver own data. In recent years, many possible applications of ad hoc networks are discussed, such as in sensor networks, conference meetings and extending of the range of base stations through the use of ad hoc networks. In these applications, the nodes do not always belong to one owner or share a common objective, as a result nodes may not be willing to route packets for other nodes for various reasons. These reasons can include commercial benefits or it may want to preserve its own battery life.

Due to the nature of the wireless medium, malicious nodes, which may not belong to any organisation, can disrupt the operations of ad hoc networks by injecting wrong routing information or injecting forged data packets. Moreover, viruses can disrupt the operations of networks by modifying the behavior of routing protocols or creating denial-of-service attacks by sending large number of forged routing or data packets into the network.

Security is a key concern in MANETs because their nodes are generally more susceptible to various threats than those in traditional wired networks. Current schemes of detecting node selfishness in MANET are mostly centered on using audit, incentives,

reputation, price or acknowledgement based mechanisms to achieve the desired effect of nodes cooperation.

Selfishness in its worse form involves a deliberate intent by a node or group of nodes to disrupt the operation of the network for its own objectives. Such nodes are termed malicious and dealing with them would involve the areas of providing security in MANETs.

CHAPTER 2

LITERATURE REVIEW

Previously proposed methods for detecting node misbehaviors can be classified into

(a) Audit based system

(b) Credit based systems

(c) Reputation based systems

(d) Acknowledgment based systems

(e) Collaborative based system

2.1 Audit Based System

Audit-based system that effectively and efficiently isolates both continuous and selective packet droppers. Yu Zhang and Loukas Lazos proposed a comprehensive system called Audit-based Misbehavior Detection (AMD) that effectively and efficiently isolates both continuous and selective packet droppers. The AMD system integrates reputation management, trustworthy route discovery, and identification of misbehaving nodes based on behavioral audits. William Kozma Jr.and Loukas Lazos proposed a novel misbehavior identification scheme called REAct that provides resource-eficient account ability for node misbehavior. REAct identifies misbehaving nodes based on a series of random audits triggered upon a performance drop.

2.2 Credit Based Systems

Credit-based systems are designed to provide incentives for forwarding packets. Buttyan and Hubaux proposed a system in which nodes accumulate credit for every packet they forward, and spend their credit to transmit their own packets. To ensure correctness, the credit counter is implemented in tamper-proof hardware. Zhong et al.

proposed Sprite, in which nodes collect receipts for the packets they forward to other nodes. When the node has a high-speed link to a Credit Clearance Service (CCS), it uploads its receipts and obtains credit. Crowcroft et al. proposed a scheme that adjusts the credit reward to traffic and congestion conditions. While credit-based systems motivate selfish nodes to cooperate, they provide no incentive to malicious nodes. Such nodes have no intend to collect credit for forwarding their own traffic. Moreover, credit-based systems do not identify misbehaving nodes, thus allowing them to remain within the network indefinitely.

2.3 Reputation Based Systems

Reputation-based systems use ratings for evaluating the trustworthiness of nodes in forwarding traffic. These ratings are dynamically adjusted based on the nodes' observed behavior. In the context of ad hoc networks, Ganeriwal and Srivastava developed a Bayesian model to map binary ratings to reputation metrics, using a beta probability density function. Jøsang and Ismail proposed a similar ranking system that utilized direct feedback received from onehop neighbors. Michiardi and Molva proposed the CORE mechanism for computing, distributing, and updating reputation values composed from disparate sources of information. Reputation-based systems use neighboring monitoring techniques to evaluate the behavior of nodes. Marti et al. proposed a scheme which relies on two modules, the watchdog and the pathrater. The watchdog module is responsible for overhearing the transmission of a successor node, thus verifying the successful packet forwarding to the next hop. The pathrater module uses the accusations generated by the watchdog module to select paths free of misbehaving nodes.

Buchegger and Le Boudec proposed a scheme called CONFIDANT, which extends the watchdog module to all one-hop neighbors that can monitor nearby transmissions (not just the predecessor node). When misbehavior is detected, monitoring nodes broadcast alarm messages in order to notify their peers of the detected misbehavior and adjust the corresponding reputation values. Similar monitoring techniques have also been used in. Transmission overhearing becomes highly complex in multichannel networks or when nodes are equipped with directional antennas. Neighboring nodes may be engaged in parallel transmissions in orthogonal channels or different sectors thus being unable to monitor their peers. Moreover, operating radios in promiscuous mode for the purpose of overhearing requires up to 0.5 times the amount of energy for transmitting a message .

2.4 Collaborative Based system

Enrique Hernandez-Orallo et al. proposed Collaborative Contact-based Watchdog (CoCoWa) as a new scheme for detecting selfish nodes that combines local watchdog detections and the dissemination of this information on the network. If one node has previously detected a selfish node it can transmit this information to other nodes when a contact occurs.

This way, nodes have second hand information about the selfish nodes in the network. Existing solutions for identifying selfish nodes either use some form of per-packet evaluation of peer behavior or provide cooperation incentives to stimulate participation. Incentivebased approaches do not address the case of malicious nodes who aim at disrupting the overall network operation. On the other hand, per-packet behavior evaluation techniques are based on either transmission overhearing or issuance of perpacket acknowledgements. These monitoring operations must be repeated on every hop of a multi-hop route, thus leading to 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS) high communication overhead and energy expenditure.

Moreover, they fail to detect dropping attacks of selective nature, since intermediate monitoring nodes may not be aware of the desired selective dropping pattern to be detected.

2.5 Secure Link State Routing for Mobile Ad Hoc Networks

The secure operation of the routing protocol is one of the major challenges to be met for the proliferation of the Mobile Ad hoc Networking (MANET) paradigm. Nevertheless, security enhancements have been proposed mostly for reactive MANET protocols. The proposed here Secure Link State Routing Protocol (SLSP) provides secure proactive topology discovery, which can be multiply beneficial to the network operation. SLSP can be employed as a stand-alone protocol, or fit naturally into a hybrid routing framework, when combined with a reactive protocol. SLSP is robust against individual attackers, it is capable of adjusting its scope between local and network-wide topology discovery, and it is capable of operating in networks of frequently changing topology and membership.

The collaborative, self-organizing environment of the Mobile Ad Hoc Networking (MANET) technology opens the network to numerous security attacks that can actively disrupt the routing protocol and disable communication. Recently, a number of

protocols have been proposed to secure the route discovery process in frequently changing MANET topologies.

These protocols are designed to perform route discovery only when a source node needs to route packets to a destination; that is, they are reactive routing protocols . Nevertheless, in many cases, proactive discovery of topology can be more efficient; e.g., in networks with low- to medium-mobility, or with high connection rates and frequent communication with a large portion of the network nodes. Furthermore, hybrid routing protocols , which are the middle ground, have been shown to be capable of adapting their operation to achieve the best performance under differing operational conditions through locally proactive and globally reactive operation.

In this paper, we study how to provide secure proactive routing and we propose a proactive MANET protocol that secures the discovery and the distribution of link state information across mobile ad hoc domains. Our goal is to provide correct (i.e., factual), up-to-date, and authentic link state information, robust against Byzantine behavior and failures of individual nodes. The choice of a link state protocol provides such robustness, unlike distance vector protocols , which can be significantly more affected by a single misbehaving node. Furthermore, the availability of explicit connectivity information, present in link state protocols, has additional benefits: examples include the ability of the source to determine and route simultaneously across multiple routes , the utilization of the local topology for efficient dissemination of data or efficient propagation of control traffic . Finally, a wide range of MANET instances is targeted by our design, which avoids restrictive assumptions on the underlying network trust and membership, and does not require specialized node equipment (e.g., GPS or synchronized clocks).

We present here our Secure Link State Protocol (SLSP) for mobile ad hoc networks, which is robust against individual attackers. SLSP shares security goals and bears some resemblance to secure link state routing protocols proposed for the “wired” Internet, but, at the same time, it is tailored to the salient features of the MANET paradigm. More specifically, SLSP does rely on the requirements of the robust flooding protocol , that is, a central entity to distribute all keys throughout the network and the reliable flooding of link state updates throughout the entire network. SLSP does not seek to synchronize the topology maps across all nodes or to support the full exchange of link state databases . Note that nodes cannot be provided with credentials to prove their authorization to advertise specific routing information due to the continuously changing network connectivity and membership.

Finally, the participation of nodes in routing does not stem from their possession of credentials , since in MANET, all nodes are expected to equally assist the network operation. First we present our assumptions and network model, followed by an overview and the definition of SLSP. Next, we discuss a number of relevant issues and conclude by describing related future work.

2.5.1 SLSP Definition

The Secure Link State Protocol (SLSP) for mobile ad hoc networks is responsible for securing the discovery and distribution of link state information. The scope of SLSP may range from a secure neighborhood discovery to a network-wide secure link state protocol. SLSP nodes disseminate their link state updates and maintain topological information for the subset of network nodes within R hops, which is termed as their zone. Nevertheless, SLSP is a self-contained link state discovery in Proceedings of the IEEE Workshop on Security and Assurance in Ad hoc Networks, in conjunction with the 2003 International Symposium on Applications and the Internet, Orlando, FL, January 28, 2003 protocol, even though it draws from, and naturally fits within, the concept of hybrid routing.

2.5.1.1 Assumptions and network model

Each node is equipped with a public/private key pair, namely EV and DV, and with a single network interface per node within a MANET domain.1 Key certification can be provided by a coalition of K nodes and the use of threshold cryptography [15,13], the use of local repositories of certificates provided by the network nodes , or a distributed instantiation of a CA.

Nodes are identified by their IP addresses, which may be assigned by a variety of schemes, e.g., dynamically or even randomly. Although EV does not need to be tied to the node's IP address, it could be beneficial to use IP addresses derived from the nodes' public keys. Nodes are equipped with a one-way or hash function H and a public key cryptosystem.

Adversaries may disrupt the protocol operation by exhibiting arbitrary malicious behavior: e.g., replay, forge, corrupt link state updates, try to influence the topology view of benign nodes, or exploit the protocol to mount Denial of Service (DoS) attacks. SLSP is concerned solely with securing the topology discovery; it does not guarantee that adversaries, which complied with its operation during route discovery, would not attempt to disrupt the actual data transmission at a later time. The protection of the data transmission is a distinct problem, which we address in a different publication.

2.5.1.2 Overview

To counter adversaries, SLSP protects link state update (LSU) packets from malicious alteration, as they propagate across the network. It disallows advertisements of non-existent, fabricated links, stops nodes from masquerading their peers, strengthens

the robustness of neighbor discovery, and thwarts deliberate floods of control traffic that exhausts network and node resources. To operate efficiently in the absence of a central key management, SLSP provides for each node to distribute its public key to nodes within its zone. Nodes periodically broadcast their certified key, so that the receiving nodes validate their subsequent link state updates. As the network topology changes, nodes learn the keys of nodes that move into their zone, thus keeping track of a relatively limited number of keys at every instance.

SLSP defines a secure neighbor discovery that binds each node V to its Medium Access Control (MAC) address and its IP address, and allows all other nodes within transmission range to identify V unambiguously, given that they already have EV. Nodes advertise the state of their incident links by broadcasting periodically signed link state updates (LSU). SLSP

1 To support operation with multiple interfaces, one key pair should be assigned to each interface. restricts the propagation of the LSU packets within the zone of their origin node. Receiving nodes validate the updates, suppress duplicates, and relay previously unseen updates that have not already propagated R hops. Link state information acquired from validated LSU packets is accepted only if both nodes incident on each link advertise the same state of the link.

2.5.1.3 Neighbor Discovery

Each node commits its Medium Access Control (MAC) address and its IP address, the (MACV, IPV) pair, to its neighbors by broadcasting signed hello messages. Receiving nodes validate the signature and retain the information; in the case of SUCV addresses the confirmation for the IP address can be done in a memory-less manner. The proposed binding of the MACV strengthens the robustness of our scheme, by disallowing nodes from appearing as multiple ones at the data link layer, and by assisting in protection against flooding DoS attacks.

To achieve these goals, we propose that the Neighbor Lookup Protocol (NLP) be an integral part of SLSP. NLP is responsible for the following tasks: (i) maintaining a mapping of MAC and IP layer addresses of the node's neighbors, (ii) identifying potential discrepancies, such as the use of multiple IP addresses by a single data-link interface, and (iii) measuring the rates at which control packets are received from each neighbor, by differentiating the traffic primarily based on MAC addresses. The measured rates of incoming control packets are provided to the routing protocol. This way, control traffic originating from nodes that selfishly or maliciously attempt to overload the network can be discarded.

Basically, NLP extracts and retains the 48-bit hardware source address for

each received (overheard) frame, along with the encapsulated IP address. This requires a simple modification of the device driver, so that the data link address is "passed up" to the routing protocol along with each packet. With nodes operating in promiscuous mode, the extraction of such pairs of addresses from all overheard packets leads to a significant reduction in the use of the neighbor discovery and query/reply mechanisms for medium access control address resolution. Each node updates its neighbor table by retaining both, the data-link and the network interface addresses addresses. The mappings between the two addresses are retained in the table as long as transmissions from the corresponding neighboring nodes are overheard; a lost neighbor timeout period2 is associated with each table entry.

NLP issues a notification to SLSP, according to the content of a received packet, in the event that: (i) a neighbor used an IP address different from the address currently recorded in the neighbor table, (ii) two neighbors used the same IP address (that is, a packet appears to originate from a node that may have 2 The lost neighbor timeout should be longer than the timeout periods associated with the flushing of routing information (link state, routing table entries), related to the particular neighbor. "spoofed" an IP address), (iii) a node uses the same medium access control address as the detecting node (in that case, the data link address may be "spoofed"). Upon reception of the notification, the routing protocol discards the packet bearing the address that violated the aforementioned policies.

2.6 A study of research trends and issues in wireless Ad hoc networks

Ad hoc network enables network creation on the fly without support of any predefined infrastructure. The spontaneous erection of networks in anytime and anywhere fashion enables development of various novel applications based on ad hoc networks. However, at the same ad hoc network presents several new challenges. Different research proposals have came forward to resolve these challenges. This chapter provides a survey of current issues, solutions and research trends in wireless ad hoc network. Even though various surveys are already available on the topic, rapid developments in recent years call for an updated account on this topic. The chapter has been organized as follows. In the first part of the chapter, various ad hoc network's issues arising at different layers of TCP/IP protocol stack are presented. An overview of research proposals to address each of these issues is also provided. The second part of the chapter investigates various emerging models of ad hoc networks, discusses their distinctive properties and highlights various research issues arising due to these properties. We specifically provide discussion on ad hoc grids, ad hoc clouds, wireless mesh networks and cognitive radio ad hoc networks. The chapter ends with presenting summary of the current research on ad hoc network, ignored research areas and directions for further research.

During last few years, extensive developments have been observed in the domain of wireless network. Different communication technologies i.e. general packet radio service (GPRS), enhanced data rates for GSM evolution (EDGE) and worldwide interoperability for microwave access (WIMAX) etc. have evolved and newer form of computing devices i.e. personal digital assistant (PDA), tablets and smart phones are appearing in the market. The wireless computing has progressed from 1G to 4G communication networks. During this progression, various modes of wireless networking have emerged. The simplest form of wireless networking is communication among two or more fixed hosts in open air. The conventional television system operates on this mode. Another approach is wireless networking with access point. There are different wireless hosts that are allowed to move while the basic infrastructure is supported by set of fixed nodes called base stations or access points. However, this approach doesn't provide the flexibility to be used in emergency situations requiring quick deployment or networking in adversarial surroundings.

The evolution of technologies has lead to development a new mode of wireless networking where the nodes arrange themselves on the fly in the form of a network without any infrastructure support.

2.6.1 Properties of ad hoc network

Formally, Ad hoc Network G(N,E) is defined as a collection of nodes N=n1,n2,n3,. connected by edges (Islam and Shaikh 2012). The nodes are usually mobile with limited capabilities, links are volatile and insecure, and there are no dedicated nodes for addressing, routing, key management and directory maintenance etc. The nodes are themselves responsible for various network operations i.e. routing, security, addressing and key management etc. It is obvious from these characteristics that network protocols and algorithm that are currently available for wired and infrastructure-less wireless networks are not suitable for ad hoc networks (Islam, Shaikh et al. 2010). For example, a conventional routing algorithm when employed for ad hoc network can suffer from loops, stale routes and other issues due to the very sharp changes in the network. Similarly, the current security solutions are based on availability of authentication servers, certification authority and other security infrastructure, which are not generally available in ad hoc network. Therefore, new solutions are required for addressing various challenges of ad hoc network. Different research efforts are underway to address various issues of ad hoc networks.

In this chapter, we provide an adequate account of these efforts. There are already some surveys available that have summarized the previous researches on ad hoc networks. For example, Dow, Lin et al. (2005) and Singh, Dutta et al. (2012) have provided a quantitative analysis of the number of research proposals appeared during last few years for addressing a particular issue of ad hoc network. Similarly, a summary of various research issues in ad hoc networks have been presented in (Chlamtac, Conti et al. 2003; Toh, Mahonen et al. 2005; Ghosekar, Katkar et al. 2010; K.Al-Omari and Sumari 2010). However, the focus of this chapter is on research pursued in ad hoc networks during recent years. The major contributions of this chapter are as follows:

• To provide a summary of various research issues in ad hoc networks and the recent approaches adopted to tackle these issues

• To investigate and report on various emerging models of ad hoc networking

• To present a comprehensive overview of issues and corresponding solutions for different ad hoc networking models i.e. ad hoc grids, ad hoc clouds, wireless mesh networks and cognitive radio ad hoc networks etc.

• To summarize the current state-of-the-art and avenues for further research Such networks are called ad hoc networks.

CHAPTER 3

DISCUSSION

Social selfishness has not been addressed before. Although many routing algorithms have been proposed for MANETs, most of them do not consider users willingness and contact opportunity of node to forward packets for all others. They may not work well since some packets are forwarded to nodes unwilling to relay, and will be dropped.

To prevent the above limitation of the existing method, there is need to develop and improve the system for investigation of selfishness and misbehavior of node in MANET. Hence the present invention introduce an assignment based selfish misbehavior detection system for mobile ad hoc networks which considers both users willingness to forward and their contact opportunity to forward packets for all others.

Wireless networks build on user nodes to form the network's routing infrastructure.

In particular, the correct forwarding behaviour of each intermediate node on a multi-hop path from the source node to the destination node is crucial for the functioning of the network. According to the above introduction the at least one forwarding node and the one or more receiving nodes represent intermediate nodes. The sending node can be an intermediate node, too. However, current secure routing solutions and misbehaviour detection mechanisms are not sufficient and mostly inapplicable in wireless networks. And also in the absence of a supporting infrastructure, wireless ad hoc networks realize end-to-end communications in a cooperative manner.

Nodes rely on the establishment of multi-hop routes to overcome the limitations of their finite communication range.

In this paradigm, intermediate nodes are responsible for relaying packets

from the source to the destination. When ad hoc networks are deployed in hostile environments (tactical networks), or consist of nodes that belong to multiple independent entities, a protocol-compliant behavior cannot be assumed. Unattended devices can become compromised and drop transit traffic in order to degrade the network performance. Moreover, selfish users may misconfigure their devices to refuse forwarding traffic in order to conserve energy.

3.1 OBJECTIVES

1. Primary object of the proposed work is to provide an assignment based selfish detection system for mobile ad hoc networks which considers both users willingness to forward and their contact opportunity to forward packets for all others.

2. Another object of the proposed work is to provide an algorithm to maintain social selfishness of node in mobile ad hoc network based on packet priority.

3. Yet another object of the proposed work is to provide an algorithm to maintain willingness of nodes and based on this willingness it will check forwarding strength of nodes.

4. Yet another object of the proposed work is to evaluate the trustworthiness of nodes using well-defined perspectives.

5. Yet another object of the proposed work is to evaluate the reputation management system.

6. Yet another object of the proposed work is to provide a system to satisfy user demands for selfishness.

Ad hoc networks enable network creation on the fly without support of any predefined infrastructure. The spontaneous erection of networks in anytime and anywhere fashion enables development of various novel applications based on ad hoc networks. However, ad hoc networks present several new challenges. Different research proposals have came forward to resolve these challenges. This chapter provides a survey of current issues, solutions, and research trends in wireless ad hoc networks. Even though various surveys are already available on the topic, rapid developments in recent years call for an updated account. The chapter has been organized as follows. In the first part of the chapter, various ad hoc network issues arising at different layers of TCP/IP protocol stack are presented. An overview of research proposals to address each of these issues is also provided. The second part of the chapter investigates various emerging models of ad hoc networks, discusses their distinctive properties, and highlights various research issues arising due to these properties. The authors specifically provide discussion on ad hoc grids, ad hoc clouds, wireless mesh networks, and cognitive radio ad hoc networks. The chapter ends with a presenting summary of the current research on ad hoc networks, ignored research areas and directions for further research.

Security issues in mobile adhoc network (MANET) are veiled by various techniques that were introduced in past decade. Owing to decentralized nature of MANET, the security issues cultivates resulting in welcoming various lethal vulnerabilities. Out of all security issues in MANET, wormhole attack is considered one of the most challenging adversarial modules that tremendously affect the communication

system in MANET. This paper presents various significant security techniques for mitigating wormhole attack in MANET. The uniqueness of this paper is that it presents a state-of-art study of existing survey papers and potentially emphasized on techniques for detection and prevention of wormhole attack in MANET. Finally, the study also highlights some of the significant findings as well as research gap that stand as prime contribution of the proposed paper.

REFERENCES

[1] C. S. R. Murthy and B. S. Manoj, “Ad Hoc Wireless Networks: Architectures and Protocols”, Prentice Hall, 2004.

[2] P. Papadimitratos and Z. J. Haas, ”Secure Link State Routing for Mobile Ad Hoc Networks,” presented at Symposium on Applications and the Internet Workshops, Orlando, FL, USA, 2003.

[3] H. Yang, H. Y. Luo, F. Ye, S. W. Lu, and L. Zhang, ”Security in mobile ad hoc networks: Challenges and solutions,” IEEE Wireless Communications, vol. 11, pp. 38-47, 2004.

[4]P. Yau and C. J. Mitchell, ”Security vulnerabilities in ad hoc networks,” presented at The Seventh International Symposium on Communication Theory and Applications,, Ambleside, Lake District, UK, 2003.