IJRSET Volume 2, Issue 5 Pages: 47-54
ISSN 2394-739X
International Journal for Research in Science Engineering and Technology

SECURE INTRUSION DETECTION SYSTEM FOR MOBILE AD HOC NETWORK

[1] Mr. C. PRAKASH, MCA, M.Phil, [2] Mr. A. YOGARAJ, M.Sc., M.Phil,
[1] Assistant Professor, [2] Assistant Professor,
[1] Department of Information Technology, [2] Department of Computer Science,
[1] Dr. N.G.P College of Arts & Science, [2] PARK'S College (Autonomous),
[1] Coimbatore – 641048. [2] Tirupur-5.

Abstract: -

Security is a primary concerns when protected communication between mobile nodes in a averse environment is the requirement. MANETs are more susceptible to be attacked as compared to the wired networks. These vulnerabilities are due to the operating principles of the MANET which cannot be changed. Securing MANET is equally important as securing fixed wired networks. Certain level of security can be obtained from the existing solutions. However, these solutions are not always necessarily suitable for wireless networks. Mobile ad hoc networks (MANETs) combine wireless communication with a high degree of node mobility. Limited range wireless communication and high node mobility means that the nodes must cooperate with each other to provide essential networking, with the underlying network dynamically changing to ensure needs are continually met. An IDS based on anomaly based intrusion detection that works by checking the behavior of the nodes was proposed to overcome some of the attacks like black hole, gray hole and flooding attacks. Generally the malicious nodes demonstrate a different behavioral pattern of all the other normal nodes. So the specified approach where a Data Transmission Quality (DTQ) function is used to determine the behavior of the nodes as malicious or legitimate is used.

Keywords: - MANET, IDS, Security, Transmission, Wireless, System.

1. INTRODUCTION

MANETs by their very nature are more vulnerable to attack than wired net-works. The flexibility provided by the open broadcast medium and the cooperativeness of the mobile devices (which have generally different resource and com-putational capacities, and run usually on battery power) introduces new security risks. As part of rational risk management we must be able to identify these risks and take appropriate action. In some cases we may be able to design out particular risks cost-effectively. In other cases we may have to accept that vulnerabilities ex-ist and seek to take appropriate action when we believe someone is attacking us. As a result, intrusion detection is an indispensable part of security for MANETs. In these cases each node consists of a host and a router on the same device. This means that the nodes form a network without the use of an external routing device. When a number of such nodes happen to be near to each other and form networks, and is called as ad-hoc network or Mobile ad hoc network (MANET). As we are aware now that MANETs do not have a fixed topology, thus every single node in the network acts as a host as well as a packet forwarding device i.e., a router. Further the nodes in a MANET can move in any direction and are allowed leave the network at any point of time. Because of the absence of a solid infrastructure these networks are cheaper to deploy but also are restrained by some factors such as battery and low processing power. Therefore, when the

network grows in size the load on every single node to forward packets to other nodes increase which takes a considerable amount of processing power.Security mechanisms are a must to be used in the wireless ad hoc networks to counter against the threats. Cryptographic mechanisms are used to provide security against certain types of attacks from external nodes but cryptography cannot provide protection against malicious internal nodes which already possess the required cryptographic keys. Thus, intrusion detection mechanisms are essential to detect these internal malicious nodes. Several events in the history have proved that intrusion prevention techniques, such as authentication and encryption are not sufficient alone. They usually serve as the first line of defense. However, as the complexity of the system increases so does the weaknesses, which creates a set of new security problems. Intrusion detection system serves as a solution to this problem and can be used as a second line of defense.In Ad Hoc networks, each node is willing to forward data to other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. This is in contrast to the infrastructure-based networks in which designated nodes, usually with custom hardware and variously known as routers, switches, hubs, and firewalls, perform the task of forwarding the data. Minimal configuration and quick deployment make Ad Hoc networks suitable for emergency situations like natural or human-induced disasters, military conflicts, emergency medical situations etc. An Ad Hoc network is formed for a purpose by participating wireless nodes and is then torn off.These networks introduced a new art of network establishment and are well suited for environments where either the infrastructure is lost or where deploying an infrastructure is not cost-effective.Unlike conventional cellular wireless mobile networks that rely on extensive infrastructure to support mobility, a wireless Mobile Ad hoc NETwork (MANET) does not need expensive base stations or wired infrastructure. Nodes within the radio range of each other can communicate directly over the wireless links, while those that are far apart use other nodes as relays. In MANETs, each host must act as a router since routes are mostly multihop. Nodes in such a network move arbitrarily, thus the network topology changes frequently and unpredictably. Moreover, the wireless channel bandwidth is limited, and the mobile nodes operate on the constrained battery power which will eventually be exhausted.Extensive research efforts have been devoted to various issues related to MANETS. Because this research focuses on the protection of MANET routing protocols, here we briefly describe existing MANET routing protocols.

1.1. Routing for Mobile Ad Hoc Networks

Many routing protocols have been proposed for MANETs. In general, these protocols could be divided into three categories: proactive, reactive, and hybrid. Proactive routing protocols (such as Destination-Sequenced Distance Vector routing protocol (DSDV) and the Wireless Routing Protocol (WRP) waste limited bandwidth by continuously maintaining the complete routing information about the whole network. They react to topology changes, even if there is no traffic. They are also called table-driven methods. The protocols in this area differ in the number of tables maintained, the information each table contains as well as the details of how they are updated. Reactive routing protocols (such as Ad hoc On-demand Distance Vector routing protocol (AODV), the Temporally Ordered Routing Algorithm (TORA), and the Dynamic Source Routing protocol (DSR) are based on demand for data transmission. They can significantly reduce the routing overhead when the traffic is lightweight and the topology changes less dramatically, since they do not need to periodically update route information and do not need to find and maintain the routes when there is no traffic. The differences among reactive routing protocols lie in the implementation of the path discovery mechanism and optimizations to it. Hybrid methods combine proactive and reactive methods to find efficient routes. ZHLS

is one example of hybrid routing protocols. In ZHLS, the whole network is divided into non overlapping zones. ZHLS is proactive if the traffic destination is within the same zone of the source. It is reactive because a location search is needed to find the zone ID of the destination.

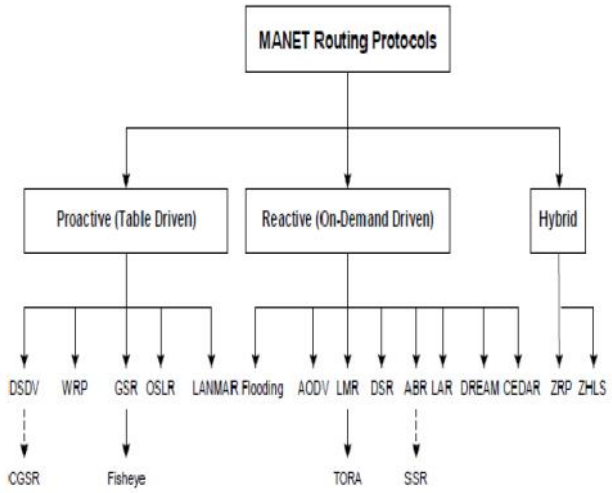

Figure 1: Classification of Routing Protocols

Fig. 1.1 is a categorization of existing routing protocols in MANETs. In the figure, solid lines represent direct descendants while dotted lines depict logical descendants. Since new routing protocols are always being proposed for MANETs, we do not expect to include all of them here.

2. ATTACKS AND THREATS IN MANET

The number of different threats and attacks can be categorized into a number of different areas that they target. The first is to consider the level of the attack which can be perceptual where the human perception is targeted using the media as a bearer. It may be broadcasting false information or just observation of social behavior to be able to alter decision processes.Secondly the attacks can target the information itself where interception and eavesdropping comes naturally in thought. Of the more active nature of these attacks might be the creation of false messages injected into networks. Also the denial or degradation of network services is a form of active attack on the information level. In this category application level attacks such as Trojan horses or viruses and the like are also included.The physical attacks are the third category. The passive nature of this category can be radiation interception or inductive wiretapping. The more hands on attacks include theft of equipment, cryptographic or physical keys, and different storage Medias.

- **Routing Loop**

By sending forged routing packets an attacker can create a routing loop.

- **Black Hole**

The setup for the black hole attack is similar to the routing loop attack in which the attacker sends out forged routing packets.

- **Grey Hole**

A special case of the black hole attack is an grey hole attack. In this attack the adversary selectively drops some kinds of packets but not other.

- **Partitioning**

Another kind of attack is for the attacker to create a network partition in which some nodes are split up to not being able to communicate with another set of nodes. By analyzing the network topology the attacker can choose to make the partitioning between the set of nodes that makes the most harm into the system.

- **Blackmail**

Some Ad Hoc routing protocols tries to handle the security problems by keeping lists of possibly malicious nodes. Each node has a blacklist of, what it thinks, bad nodes and thereby avoiding using them when setting up routing paths.

- **Wormhole**

In the wormhole attack an attacker uses a pair of nodes connected in some way. It can be a special private connection or the packets

are tunneled over the Ad Hoc network. Every packet that one of the nodes sees are forwarded to the other node which in turn broadcast them out.

- **Rushing Attack**

Many reactive routing protocols keep a sequence number for duplication suppression at every node. An attacker can distribute a large number of route requests with increasing sequence numbers forged to appear to be from other nodes.

- **Resource Consumption**

By injecting extra data packets into the Ad Hoc network limited resources such as bandwidth and maybe battery power are consumed for no reason. Even more resources might be consumed by injecting extra control packets since these might lead to additional computation.

- **Dropping Routing Traffic**

It is essential in the Ad Hoc network that all nodes participate in the routing process.

- **Location disclosure**

A location disclosure attack can reveal information related to the location of a node or the topology and structure of the network. Because of dynamic topological changes, ad-hoc networks are vulnerable at the physical link, as they can easily be manipulated. An intruder can easily attack ad-hoc networks by loading available network resources, such as wireless links and energy (battery) levels of other users, and then disturb all users. Attackers can also disturb the normal operation of routing protocols by modifying packets. The intruder may insert spurious information into routing packets, causing erroneous routing table updates and thus misrouting.

3. INTRUSION DETECTION SYSTEM (IDS)

Intrusion is any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource and an intrusion detection system (IDS) is a system for the detection of such intrusions. There are three main components of IDS: data collection, detection, and response. The data collection component is responsible for collection and pre-processing data tasks: transferring data to a common format, data storage and sending data to the detection module. IDS can use different data sources as inputs to the sys-tem: system logs, network packets, etc. In the detection component data is ana-lyzed to detect intrusion attempts and indications of detected intrusions are sent to the response component. In the literature, three intrusion detection techniques are used. The first tech-nique is anomaly-based intrusion detection which profiles the symptoms of nor-mal behaviors of the system such as usage frequency of commands, CPU usage for programs, and the like. It detects intrusions as anomalies, i.e. deviations from the normal behaviors. Various techniques have been applied for anomaly detection, e.g. statistical approaches and artificial intelligence techniques like data min-ing and neural networks. Defining normal behavior is a major challenge. Normal behavior can change over time and intrusion detection systems must be kept up to date. False positives – the normal activities which are detected as anomalies by IDS – can be high in anomaly-based detection. On the other hand, it is capable of detecting previously unknown attacks. This is very important in an environment where new attacks and new vulnerabilities of systems are announced constantly.Misuse-based intrusion detection compares known attack signatures with cur-rent system activities. It is generally preferred by commercial IDSs since it is efficient and has a low false positive rate. The drawback of this approach is that it cannot detect new attacks. The system is only as strong as its signature database and this needs frequent updating for new attacks. Both anomaly-based and misuse-based approaches have their strengths and weaknesses. Therefore, both techniques are generally employed for effective intrusion detection. The last technique is specification-based intrusion detection. In this approach, a set of constraints

on a program or a protocol are specified and intrusions are detected as runtime violations of these specifications. It is introduced as a promising alternative that combines the strengths of anomaly-based and misuse-based detection techniques, providing detection of known and unknown attacks with a lower false positive rate. It can detect new attacks that do not follow the system specifications. Moreover, it does not trigger false alarms when the program or protocol has unusual but legitimate behavior, since it uses the legitimate specifications of the program or protocol. It has been applied to ARP (Address Resolution Protocol), DHCP (Dynamic Host Configuration Protocol) and many MANET routing protocols. Defining detailed specifications for each pro-gram/protocol can be a very time consuming job. New specifications are also needed for each new program/protocol and the approach cannot detect some kind of attacks such as DoS (Denial of Service) attacks since these do not violate pro-gram specifications directly. Different characteristics of MANETs make conventional IDSs ineffective and inefficient for this new environment. There are new issues which should be taken into ac-count when a new IDS is being designed for MANETs.

- Lack of Central Points.
- Mobility.
- Wireless Links.
- Limited Resources.
- Cooperativeness,

Mobile Ad Hoc Networks (MANETs) present a number of unique problems for Intrusion Detection Systems (IDS). Differentiating between malicious network activity and spurious, but typical, problems associated with an Ad Hoc networking environment is a challenging task. In an Ad Hoc network, malicious nodes may enter and leave the immediate radio transmission range at random intervals or may collude with other malicious nodes to disrupt network activity and avoid detection. Malicious nodes may behave maliciously only intermittently, further complicating their detection. A node that sends out false routing information could be the one that has been compromised, or merely one that has a temporarily stale routing table due to volatile physical conditions. Dynamic topologies make it difficult to obtain a global view of the network and any approximation can become quickly outdated. Traffic monitoring in wired networks is usually performed at switches, routers and gateways, but an Ad Hoc network does not have these types of network elements where the IDS can collect audit data for the entire network. Network traffic can be monitored on a wired network segment, but Ad Hoc nodes or sensors can only monitor network traffic within its observable radio transmission range. NIST is working with the University of Maryland Baltimore County (UMBC) to simulate, implement, and test various MANETs IDS.

4. PROPOSED SYSTEM & ITS IMPLEMENTATION

The mobile nodes interacting together in a MANET should co-operate together and share resources and wireless capabilities in order to enable end-to-end communication. The work of routers is performed by the intermediate nodes so as to increase the connectivity of the peers which are not in the radio range of each other. It can be attained by efficiently transmitting messages in a multihop transmission scheme which is determined by an ever changing routing through the radio channel. Due to the mobile nature of the hosts the MANET scenario taken as a disturbing system for routing protocols. There are various routing protocols which have been proposed for this type of scheme such as AODV, DSDV, DSR, and OLSR. However most of these protocols use the cooperative nature of the hosts as an assumption: but this may not be always feasible in real time systems. In our work, a hybrid routing protocol has been designed based on AODV which incorporates the IDS functionalities in itself. This new routing protocol is called as Intrusion Detection System based AODV (ISAODV). It is developed by integrating an IDS with the

concept of SUCV identifiers, for MANETs based on IPv6. SUCV identifiers fulfill the need of having a trusted Certification Authority or Key Distribution Center by providing a protected binding between the IP addresses of the nodes and the cryptographic values.

4.1 System Design

A MANET can be supposed as a group of cooperative nodes which utilize a common routing protocol. Here we consider the specifications of the routing protocol to be the normal activity of the system. Nodes which deviate from this defined normal behavior are considered as malicious. Thus, the given anomaly-based IDS works for detecting several attacks by describing an intrusion as a deviation from the defined normal behavior.

The two major components of the defined mechanism are as follows:

1) An host and anomaly based IDS mechanism with passive reactions.

2) The Statistically Unique and Cryptographically Verifiable (SUCV) identifiers,In order to provide a protection bond between the IP and public key without the requirement of any certification authority and key distribution center. The goal of our approach is to find a secure route between the source and destination nodes. We also aim to provide scalability and actability to our system by implementing clustering algorithm which ultimately emerges in an secure cluster with only the safe nodes being part of it. In order to obtain our goals we first need to find safe routes and then maintain the route obtained.In order to implement the proposed mechanism in MANET following assumptions are made:

1) The source and destination nodes are considered safe.

2) The nodes share a bidirectional link.

3) The nodes are able to hear the neighbour's transmission.

4) All nodes except the malicious ones have IDS activated on them.

5) A hash function is distributed with the system configuration setting to all the participating nodes in the network.

6) The MANET is homogeneous.

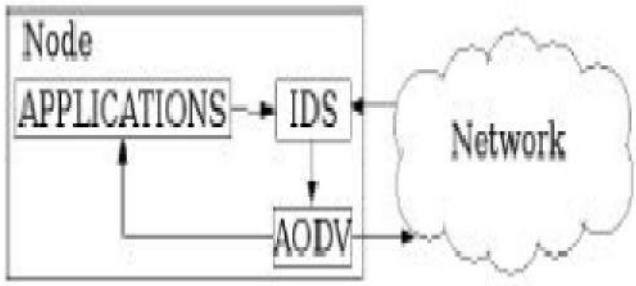

Figure 2: The Proposed Structure

All the traffic owing through the MANET is occupied by the IDS and for processing by the AODV routing protocol these packets are also altered by the IDS. Each bundle accepted by contiguous hubs throughout a way disclosure methodology is checked, to check if the parcel is sent by an at one time recognized vindictive hub. Each packet accepted by the following nodes in a predefined way, is checked to confirm in the event that it has been undermined. In both cases the packet is quickly eliminated. At the end of the day, malicious hosts are avoided from the ways they endeavor to attack.

5. IMPLEMENTATION & RESULTS

In order to evaluate the performance of the system, we simulated a model of MANET on the ns2 simulator. The IS-AODV model has been derived from the AODV model provided with the ns2 simulator. We have modified the AODV according to the proposed mechanism.

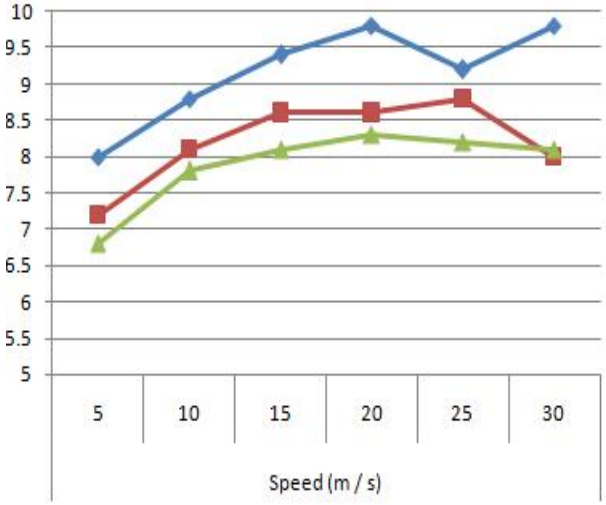

Figure 3: Total Overhead

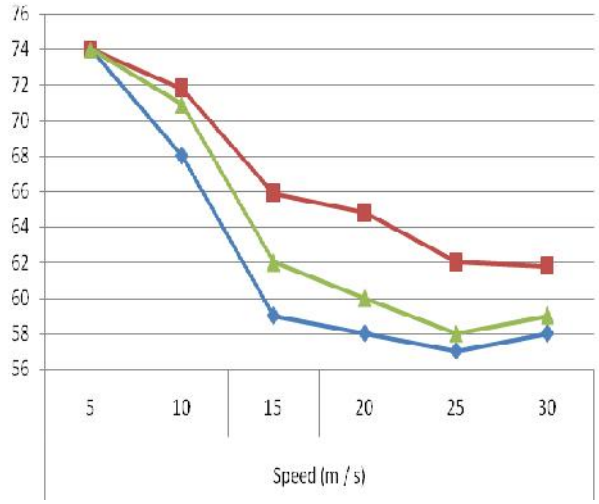

Figure 4: Delivery Ratio

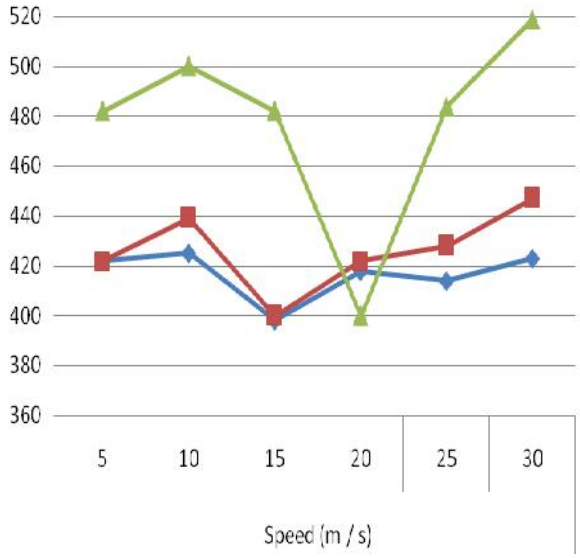

Figure 5: Network Lifetime Vs Speed

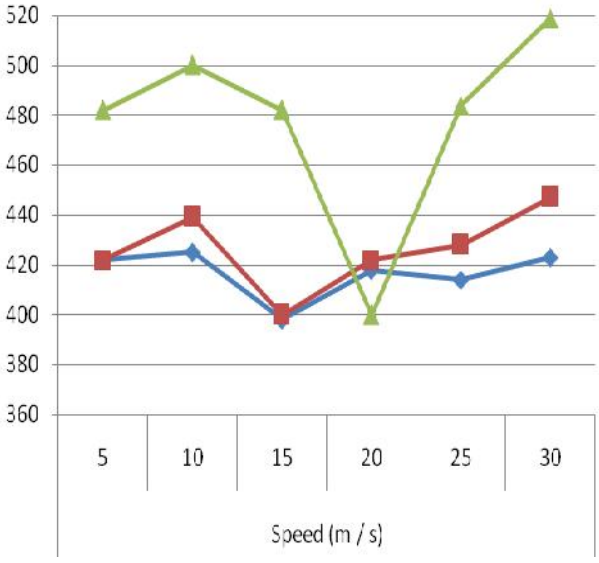

Figure 6: End-to-End Delay

This process is repeated by every selected forwarding node, except the destination node. Non-forwarding nodes drop received route request packets. Thus, the forwarding nodes are selected dynamically in an expanding ring fashion starting with the source. At each step, the selection process has for goal reducing the number of upcoming forwarding nodes. Using extensive simulations, we have evaluated the proposed schemes and found that they have very low overhead, yet they can achieve substantially higher delivery ratios than AODV when the traffic load is heavy. Even under moderate loads, they can achieve slightly higher delivery ratios than AODV, which is a successful and well-known routing scheme for ad hoc networks.

CONCLUSION

An Intrusion Detection System aiming at securing the AODV protocol has been developed using specification-based technique. It is based on a previous work done by Stamouli et al. The IDS performance in detecting misuse of the AODV protocol has been discussed. In all the cases, the attack was detected as a violation to one of the AODV protocol specifications. From the results obtained, it can be concluded that our IDS can effectively detect Sequence Number Attack, Packet Dropping Attack and Resource Depletion Attack with Incremental Deployment. The method has been shown to have low overheads and high detection rate. Simulation results confirmed that the proposed IDS contribute to a transparent clustering of nodes which eliminate the attackers with a passive reaction. Further using the PMW clustering algorithm, we were to obtain greater stability of the clustering by reducing the number of times the rescheduling was being performed otherwise. Simulation results validate the ability of our protocol to successfully detect both local and distributed attacks against the AODV routing protocol, with a low number of false positives.

REFERENCES

[1] Perkins, C.E. and Bhagwat, P. "Highly Dynamic Destination-Sequenced distance-vector routing (DSDV) for mobile computers", ACMSIGCOMM Computer Communication Review, vol. 24, no. 4, pp. 234-244, 1994.

[2] Qayyum, A., Jacquet, P. and Muhlethaler, P. "Optimized Link State Routing Protocol (OLSR)", 2003.

[3] Ogier, R., Templin, F. and Lewis, M. (2004) Topology dissemination based on reversepath forwarding (TBRPF), 2004.

[4] Das, S., Perkins, C. and Royer, E. "Ad hoc on demand distance vector (AODV) routing", Mobile Ad-hoc Network (MANET) Working Group, IETF, 2002 .

[5] Johnson, D.B., Maltz, D.A. and Broch, J. "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks", Ad hoc networking, vol. 5, pp. 139-172, 2001.

[6] Z. J. Haas, M. R. Pearlman, and P. Samar, "The Zone Routing Protocol (ZRP) for ad hoc networks," IETF Internet Draft, draft-ietf-manet-zonezrp-04.txt., July 2002.

[7] Tseng, Y.C., Ni, S.Y., Chen, Y.S. and Sheu, J.P. "The broadcast storm problem in a mobile ad hoc network", Wireless networks, vol. 8, no. 2, pp. 153-167, 2002.

[8] Abdulai, J., Ould-Khaoua, M. and Mackenzie, L. "Improving probabilistic route discovery in mobile ad hoc networks", Local Computer Networks,. 32nd IEEE Conference, pp. 739, 2007.

[9] Y.-C. Tseng, S.-Y.Ni, and E.-Y. Shih, "Adaptive approaches to relieving broadcast storms in a wireless multihop mobile ad hoc networks," Proceedings of IEEE Transactions on Computers, vol. 52, pp. 545--557, May 2003.

[10] B. Williams and T. Camp, "Comparison of broadcasting techniques for mobile ad hoc networks," Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing, MOBIHOC, pp. 194 - 205, June 2002.

[11] Le, T.D. and Choo, H. "Efficient flooding scheme based on 2-hop backward information in ad hoc networks", IEEE ICC'08 International Conference on Communications, pp. 2443, 2008.

[12] Yang, S.R., Chiu, C.W. and Yen, W.T. "A novel convex hull-based flooding scheme using 1-hop neighbour information for mobile ad hoc networks", Wireless Networks, vol. 17, no. 7, pp. 1715-1729, 2011.

[13] Liu, H., Wan, P., Jia, X., Liu, X. and Yao, F. "Efficient flooding scheme based on 1-hop information in mobile ad hoc networks", Proc. IEEE INFOCOM, 2006.

[14] Lee, S.H. and Ko, Y.B. "An Efficient Neighbor Knowledge Based Broadcasting for Mobile Ad Hoc Networks", Computational Science–ICCS, pp. 1097-1100, 2006.

[15] Abolhasan, M. and Wysocki, T. "GPS-based route discovery algorithms for on demand routing protocols in MANETs", Wireless On-Demand Network Systems, pp. 144-157, 2004.