Suresh Gyan Vihar University, Jaipur
International Journal of Converging Technologies and Management (IJCTM)
Volume 1, Issue 1, 2015
ISSN : 2455-7528

Delayed Data Packet Attack on Reactive Routing in TCP/FTP and UDP/CBR -based MANETs

Sunny Bansal [1]
[1]M.Tech Scholar, Suresh Gyan Vihar University
[1]sunny.b8591@gmail.com Dr.
Dinesh Goyal [2]
[2]Associate Professor, Suresh Gyan Vihar University
[2]Dgoyal@Gyanvihar.org

abstract: Ad-hoc On-demand Distance Vector (AODV) routing protocol is one example of such protocols. It is very popular and used very vastly. But the traditional AODV is not able to provide any QoS support to any traffic it is routing. On the other hand, today's delay and bandwidth sensitive multimedia applications required some sort of QoS provisioning for efficient and reliable transmission over wireless network.

In this work, we measure the effects of this attack on closed loop protocols such as TCP/FTP as well as CBR/UDP to find out the impact factor of this attack on network throughput, end-to-end delay and number of retransmissions.

Keyword: *Data Packet, TCp,UDP,CBR,MANET*

Introduction

In the past few years, wireless communication has grown very quickly. The best feature provided by such networks is no wires. Users can take away handheld devices anywhere with them. They get benefited from small devices, long lasting batteries.

High bandwidths are available from new communication standards. In order to communicate via such a network, fixed infrastructure is not necessary. These self organizing networks (Ad hoc networks) have gained interest on a large scale in recent times. The most common applications of wireless networks are Group Standard for Mobile communications (GSM) and Wireless Local Area Net- work (WLAN). Nodes are not arranged in any particular fashion in such networks. So to ensure better communication in between nodes, some routing protocols have been developed for such networks. These protocols also help to utilize the re-sources optimally.

At network level, the routing protocol has to guarantee that a node can be reached from any other node in the network. This objective is difficult to achieve because of the presence of both wireless links and mobile nodes, which call for dynamic reconfiguration of the routing strategy as soon as network connectivity changes. The classical linkstate and distance vector routing protocols are not suitable in such case, since they have not been designed for mobile devices with limited resources and which communicate through wireless links. For this reason, a number of routing protocols specifically devised for MANETs have been proposed in the last years, and some of them have been standardized by the Internet Engineering Task Force (IETF). Such protocols can be roughly classified in three categories: proactive, reactive and hybrid. With proactive protocols (also named tablebased) each node maintains information enabling it to decide how to route messages towards any other node in the network. Such information is usually stored in a certain number of tables (updated over time) providing each node with a view of the network topology. Differences among these protocols reside in the way the topology information is detected and updated, as well as in the type of information that is stored in each such table. Protocols falling in this category do not work efficiently when the topology changes quickly and the number of nodes is high. In fact, network changes require time to be spread among the nodes, and the amount of information to store and update grows linearly with the size of the network. On the other hand, proactive protocols guarantee to find the forwarding path in a very short time, because all the

necessary information is already available when data have to be transmitted. Moreover, they allow to find, in a simple way, a path based on specific QoS requirements. Destination- Sequenced Distance Vector (DSDV) and Optimized Link State Routing (OLSR) are probably the most well known proactive protocols available nowadays. With reactive protocols (also named on demand protocols) a path discovery process is started from a source which wants to transmit a packet towards a specific destination. The name 'on demand' is due to the fact that the search of a suitable forwarding path takes place only when data transmission is needed. Once a node determines a route, it will maintain this route for the entire duration of the transmission. In the discovery process of a route towards a destination, the source sends route request messages through flooding. Nodes which know how to reach the required destination send back route reply messages; this message exchange phase goes on until the entire route is defined. The basic principle of reactive protocols enables a smaller overhead, because nodes only maintain information about active routes, instead of keeping in memory an updated view of the overall network. For this reason, they are suitable for highly dynamic networks. Their major drawback clearly resides in the transmission delay incurred when new data have to be transmitted. Ad-hoc On-demand Distance Vector routing (AODV) and Dynamic Source Routing (DSR) currently represent the most widely spread reactive protocols available for MANETs.

ROUTING IN MOBILE AD HOC NETWORKS

Ad hoc networks are wireless networks without a fixed infrastructure, which are usually assembled on a temporary basis to serve a specific deployment such as emergency rescue or battlefield communication. They are especially suitable for scenarios where the deployment of an infrastructure is either not feasible or is not cost effective. The differentiating feature of an ad hoc network is that the functionality normally assigned to infrastructure components, such as access points, switches, and routers, needs to be achieved by the regular nodes participating in the network. For most cases, there is an assumption that the participating nodes are mobile, do not have a guaranteed uptime, and have limited energy resources.

Before describing the types of approaches and example protocols, it is important to explain the developmental goals for an ad hoc routing protocol so that the design choices of the protocols can be better understood. Hence, the following are typical design goals for ad hoc network routing protocols:

- **Minimal control overhead:** Control messaging consumes bandwidth, processing resources, and battery power to both transmit and receive a message. Because bandwidth is at a premium, routing protocols should not send more than the minimum number of control messages they need for operation, and should be designed so that this number is relatively small. While transmitting is roughly twice as power consuming as receiving, both operations are still power consumers for the mobile devices. Hence, reducing control messaging also helps to conserve battery power.
- **Minimal processing overhead.** Algorithms that are computationally complex require significant processing cycles in devices. Because the processing cycles cause the mobile device to use resources, more battery power is consumed. Protocols that are lightweight and require a minimum of processing from the mobile device reserve battery power for more user-oriented tasks and extend the overall battery lifetime.
- **Multihop routing capability.** Because the wireless transmission range of mobile nodes is often limited, sources and destinations may typically not be within direct transmission range of each other. Hence, the routing protocol must be able to discover multi hop routes between sources and destinations so that communication between those nodes is possible.
- **Dynamic topology maintenance.** Once a route is established, it is likely that some link in the route will break due to node movement. In order for a source to communicate with a destination, a viable routing path must be maintained, even while the intermediate nodes, or even the source or destination nodes, are moving. Further, because link breaks on ad hoc networks are common, link breaks must be handled quickly with a minimum of associated overhead.
- **Loop prevention.** Routing loops occur when some node along a path selects a next hop to the destination is also a node that occurred earlier in the path. When a routing loop exists, data and control packets may traverse the path multiple times until either the path is fixed and the loop is eliminated, or until the time to live (TTL) of the packet reaches zero. Because bandwidth is scarce and packet processing and forwarding is expensive, routing loops are extremely wasteful of resources and are detrimental to the network. Even a transitory routing loop will have a negative impact on the network. Hence, loops should be avoided at all times.

Related Works and Background of Attacks on MANETs

Suresh Gyan Vihar University, Jaipur
International Journal of Converging Technologies and Management (IJCTM)
Volume 1, Issue 1, 2015
ISSN : 2455-7528

a) **Worm-Hole attack [27]:** This attack is one of the most serious attacks on MANETs. In worm hole attack at least two attackers are required to perform the attack very effectively. These two attackers resides on different areas of the network makes a tunnel through the network to communicate with each other. The attackers broadcast the wrong information to the other nodes in the network that the destination is only one hop away from them. Sometimes they also broadcast the wrong information that they are true neighbors of each other due to this the attacker one which is near to source node is easily selected on the route between the source destination pair when the route is discovered on the basis of lowest number of hops on the route. It is very difficult to detect the worm hole attack as it is not modifying any data packet or generating any false traffic in the network. The worm hole attack can be classified in three forms: a) Closed loop attack: In this type of worm hole attack the source and destination node will thinks that they are directly connected to each other because of the attackers are invisible for the source and destination nodes.

b) Half open loop: in this kind of worm hole attack either the source has one visible attacker or the destination has one visible attacker but not both and, c) Fully open attack: In this form of worm hole attack both the attackers are visible for the source and destination that is one attacker is visible on source side and one is visible at destination side. The Figure 3.1 given below shows all the above mentioned three kinds of worm hole attacks. Many solutions are proposed in the literature to detect and avoid the worm hole attacks in MANETs as given in [28] [29].

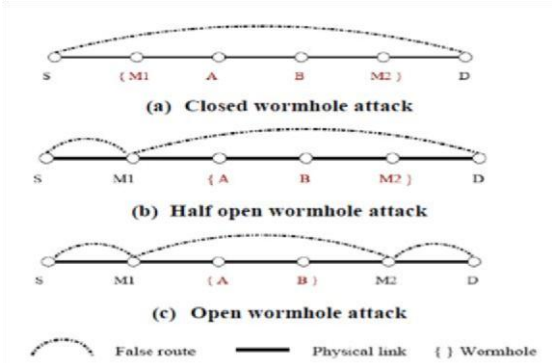


Figure 1 Classification of wormhole attacks in MANETs

b) **Black hole attack [10]:** In this attack, the attacker when received a route request (RREQ) message it modifies the sequence number in the RREQ message to perform the attack. The attacker increases the sequence number more than the usual number and reply back to the source to make it believe that it has the better and fresher route to the destination node. Once the source node got this reply it start the transmission of data packet on the route which consists of the attacker i.e., one of the intermediate node of the established route is the attacker. Till now half of the attack is performed by the attacker by spreading the false information and making himself the part of the route. Now when the data communication is started using the route the attacker will drop all the data packets that reaches to it that is when the attacker got the data packet for forwarding it drops the packet without forwarding any of the data packets. In the literature many solutions are given to detect and then avoid the black hole attack. The most efficient solutions provided are [30]. Another attack which is very close to the black hole attack in its implementation and attacking process is known as gray hole attack [31]. In this attack the attacker does not try to be get on to the path between the source destination node but it also does not forward any data packets that goes through it.

c) **Flooding attack [11]:** Flooding attack is the simplest attack to implement but it is one of the most dangerous attacks. In this attack, the attacker broadcast the false control or data packets in the network due to which the network bandwidth is wasted largely and the non-false packets are not able to reach their destinations. This attack is implemented on the reactive protocols by broadcasting the false data packets and RREQ messages. On the other hand, this attack can also be implemented on proactive routing protocols when the attacker node uses lower time to send the periodic updates. The methods to detect and avoid such nodes from the network are given in the work [32] [33].

d) **Selfish or misbehaving node attacks [12]:** As the communication in MANETs is multihop therefore the intermediate nodes plays an important role in data communication over MANETs. The intermediate nodes can become selfish by either using the wireless channel unnecessary due to which the other nearby channels has to contend more time to access the channel. The misbehaving node can change its

backoff timer used for resolve the contention and then always get the access to the channel and waste the time and channel bandwidth by not using it. The other way in which a mobile node can behave selfishly is by not forwarding any data packets or control packets it receives to forward to other nodes**.** The selfish node can do this to save its own resources so that it can use them when required later. In this kind of attack the node is not dropping any packets or generating unnecessary to harm the network intensely but still it causes damage to the network by not taking part in a network which only functions correctly or efficiently when all the nodes in the network cooperate in the routing and data communication process.

e) **JellyFish Attack [2]:** In JellyFish attack the attacker mainly tries to maximize its impact on the closed loop protocols such as TCP/FTP or CBR/UDP. In this attack the attacker drops a random amount of packets that comes to the attacker over a selected amount of time before forwarding them to the destination node. Due to this behavior of the attacker the retransmission time out (RTO) occurs at the TCP/FTP or CBR/UDP sender and it has to sent the lost packet or all packets upto the lost packet based on the sliding window algorithm that it is using for flow and congestion control. Also the numbers of duplicate ACKs sent by the destination node upon the reception of the out of the order packets are increases in the network. Due to these unnecessary packets the network bandwidth is wasted as well as the throughput of the network decreases.

PROPOSED WORK

The attack that we are implementing in this paper is named as Advisedly Delaying Packet (ADP) attack. This is because the attackers are randomly delaying few or all packets from the packets they receive for forwarding towards the destination node. We measure the effects of this attack on closed loop protocols such as TCP/FTP as well as CBR/UDP to find out the impact factor of this attack on network throughput, end-to-end delay and number of retransmissions.

Simulation Results and Performance Analysis

In this section, we present the detailed performance analysis and impact analysis of the proposed Advisedly Delaying Packet (ADP) attack on different variants of TCP protocol over mobile ad-hoc networks. The network scenarios used in the simulation process are designed in such a way so that the effects of the wireless channel and environment can be mitigated. This is done to discover the exact impact of dropping attack on the TCP-based MANETs. Therefore, we ignore the congestion and mobility induced situation from the network scenarios used for simulation process. As already mentioned above that the network simulator used for the simulation process is the trail version of the well knows network simulator called EXata [35]. The source destination pairs in the simulated network are chosen in the way it is required to ensure the full network connectivity and lowest possible environmental effects. The other network parameters used for the scenario creation with their values used during the simulation are given in Table 4.1 given below. All the results presented in this thesis are the average of 5 simulation runs calculated using different seed values.

Fig 2 Simulation Parameters

Effects of increase in packet delayed period In figure 3, we have shown the effects on network throughput for three variants of TCP protocol (mentioned above) when the attacker increases its delay period time. As it can be seen from Figure 3 that the throughput of the network decreases with the increase in the delay period time because as the delay period of the data communication increases the number of data packets that are delayed intentionally instead of forwarding them without introducing any delay by the attacker also increases. Due to this, the number of re-transmissions on the source TCP increases due to the RTO timeouts caused for the delayed data packets this further decreases the overall network throughput. Due to the delayed data packets reached at the destination node it ACKs it

Parameters	Values
Simulator	EXata
Network Size	800 x 800 meter square
Simulation time	700 Seconds
Application Layer Process	Generic File transfer protocol (FTP)
Transport Layer Protocols	TCP/FTP and CBR/UDP
Routing protocol	AODV
Number of Nodes	30
Mobility model	None
MAC specification	IEEE 802.11
Network Bandwidth	12 Mbps
Performance Metrics	Network Throughput, End-to-End Delay and Number of Retransmissions
PHY Specification	802.11a/g

later then its usual time and the TCP source might get the delayed ACK after the RTO for that data packet is expired. Due to this, TCP source is sending more duplicate data packets through the re-transmission which does not contributed in the send data packets and decreases the network throughput.

As it can also be seen from the figure 4.6 that the throughput of both the TCP/FTP and CBR/UDP protocols are decreasing with increase in the drop percentage due to delay. For every ACK that makes partial progress in the sequence space, the sender assumes that the ACK points to a new hole, and the next packet beyond the ACK ed sequence number is sent.

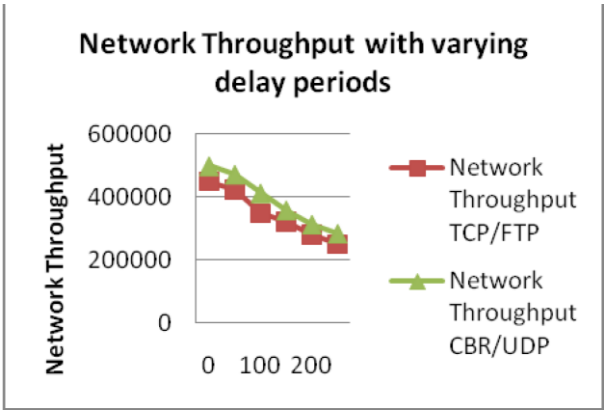


FIG 3 Throughput with increase in delayed period time of attackers (TCP/FTP and CBR/UDP based MANET scenario)

Figure 5 shows the effects of increase in the number of attackers on the route used for communication between source and destination nodes. The effect is monitered on all the three TCP variants used for the comparision in this thesis.As we can observe from Figure 4.8 that as the number of attacker increases the network throughput decreases this is becauce with the increase in the number of attackers the commulative delay of the data packet to reach to its destiantion also increases. Due to this the receiver receives the data packet later than the normal time and it sends ACKs which when reaches the source TCP the retransmission timeout for that packet is already triggered their. Therefore, the source TCP has to send the same packet and also has to go to the

slowstart and fast recovery phase which makes the TCP

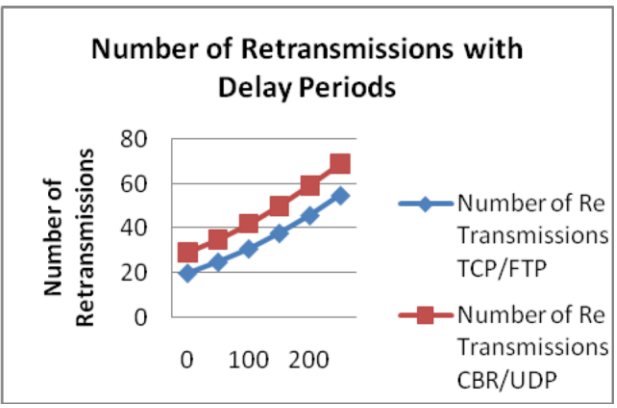


FIG 4 Number of retransmissions with increase in percentage drop time of attackers (TCP/FTP and CBR/UDP based MANET scenario)

Effects of increase in number of attackers in the route

source to send less number of data packets in the network at a given time than the actual remaining capacity of the network.

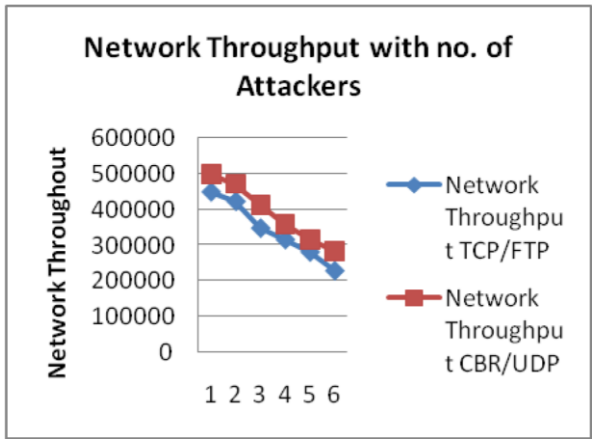
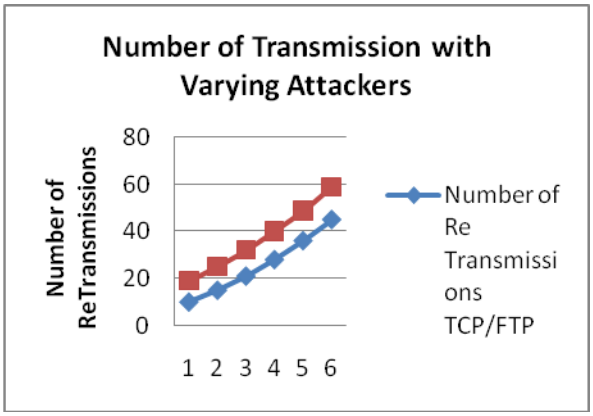


FIG 6 Number of retransmissions with increase in number of attackers on the route (TCP/FTP and CBR/UDP -based MANET scenario)

FIG 5 Throughput with increase in number of attackers on the route (TCP/FTP and CBR/UDP-based MANET scenario)



Conclusion and Future Work

We present the conclusion of the paper that we have derived based on the theoretical and simulation results. To perform the work proposed in this thesis we start with the basics of the mobile ad-hoc networks. We have studied about the MANETs and its characteristics and its challenges and issues that are faced by the researchers when performing the routing over these networks. After the in-depth introduction of MANETs we started the related work which is similar to our proposed work in this thesis. For this we have studied all forms of existing attacks over Mobile ad-hoc networks. As it can be easily seen from the work presented in Chapter 4 that the proposed Advisedly Delaying Packet (ADP) attack is a simple yet very powerful denial of service (DoS) attack that is effective on both TCP/FTP and CBR/UDP based MANETs. The simulation results clearly show the impact of proposed attack on the network throughput, bandwidth wastage and end-toend delay data quality. It has also been observed that even though the TCP/FTP and CBR/UDP congestion control is adaptable to the packet losses but in case of the forced delayed attack it is fully unable to detect whether the packet is dropped or delayed and these are the result of the attacker misbehaving or it is due to the congestion or other wireless environmental problem.

The simulation results presented in the previous chapter shows that the proposed attack is successful and it will cause the various forms of problems during the data communication process. We have checked the impact of the proposed attack on two different protocols of the TCP/IP stack (i.e., TCP/FTP and CBR/UDP) and it has been found that both the variants of the TCP/IP stack are performing poor under the attack situations. Although, if compared with each other than the TCP/FTP outperforms the other compared CBR/UDP protocol. This is because the TCP- NewReno uses the approach which uses a hybrid congestion avoidance mechanism which recovers faster when data packets are lost due to the congestion.

For the future work, we will try to discover a detection mechanism of our proposed attack in this thesis. Once detected the source node or network has to make sure

that this attacker will not become the part of any active routes in the network. Furthermore, the detection method should be fast in the way that it will detect the attack within the least duration possible from the time it has been launched. Also, we will try to figure out the other closely related attacks that can be possible to induce by a simple modification on our attack.

References

[1] A.K. Abdelaziz, M. Nafaa, and G. Salim. Survey of routing attacks and countermeasures in mobile ad hoc networks. In Computer Modelling and Simulation (UKSim), 2013 UKSim 15th International Conference on, 2013.

[2] R.H. Jhaveri, S.J. Patel, and D.C. Jinwala. Dos attacks in mobile ad hoc networks: A survey. In Advanced Computing Communication Technologies (ACCT), 2012 Second International Conference on, 2012.

[3] C. Perkins and E. Royer. Ad hoc on-demand distance vector routing. 1999.

[4] T. Socolofsky and C. Kale. a tcp/ip tutorial, ietf rfc 1180. January 1991.

[5] V. Jacobson. modified tcp congestion control and avoidance algorithms. April 1999.

[6] S. Floyd M. Mathis and A. Romanow. tcp selective acknowledgements options, ietf rfc 2018. October 1996.

[7] S. Floyd and T. Henderson. the newreno modification to tcps fast recovery algorithm, ietf rfc 3782. October 1999.

[8] SCALABLE NETWORK TECHNOLOGIES. http://www.scalable-networks.com/content/ products/ exata/.

[9] Hoang Lan Nguyen and Uyen Trang Nguyen. A study of different types of attacks in mobile ad hoc networks. In Electrical Computer Engineering (CCECE), 2012 25th IEEE Canadian Conference on, 2012.

[10] A. Mishra, R. Jaiswal, and S. Sharma. A novel approach for detecting and eliminating cooperative black hole attack using advanced dri table in ad hoc network. In Advance Computing Conference (IACC), 2013 IEEE 3rd International, 2013.

[11] Yih Chun Hu Adrian Perrig and David B. Johnson. Ariadne. a secure on-demand routing protocol for ad hoc networks. In Eighth ACM International Conference on Mobile Computing and Networking(MobiCom 2002), September 2002.

[12] M.T.Refaei V.Srivastava L.Dasilva and M.Eltoweissy. A reputation-based mechanism for isolating selfish nodes in ad hoc networks. In International Conference on Mobile and Ubiquitous Systems, Networking and Services, July 2005.

[13] W. Stevens. tcp slow start, congestion avoidance, fast retransmit, and fast recovery algorithms. Januray 1997.

[14] A. Kuzmanovic and E. Knightly. low-rate tcptargeted denial of service attacks (the shrew vs. the mice and elephants). August 2003.

[15] V.Paxson and M.Allman. computing tcps retransmission timer, ietf rfc 2988. November 2000.

[16] Imad Aad Jean Pierre Hubaux and Edward W.Knightly. denial of service resilience in ad hoc networks. September 2004.

[17] Chakrabarti, S., Mishra, A.: QoS issues in ad hoc wireless networks. Communications Magazine, IEEE 39, 142–148 (2001)

[18] Chen, S., Nahrstedt, K.: Distributed qualityofservice routing in ad hoc networks. Selected Areas in Communications, IEEE Journal 17, 1488–1505 (1999)

[19]IEFT, MANET Working Group Charter, http://www.ietf.org/html.charters/manet-charter.html.

[20] Zeadally, Sherali and Hunt, Ray and Chen, YuhShyan and Irwin, Angela and Hassan, Aamir," Vehicular ad hoc networks (VANETS): status, results, and challenges", Telecommunication Systems, Springer US, 2012.

[21] Mehran Abolhasan, Tadeusz Wysocki, Eryk Dutkiewicz, A review of routing protocols for mobile ad hoc networks, Ad Hoc Networks, Volume 2, Issue 1, January 2004.

[22] Johnson, D., Hu, Y., Maltz, D.: The dynamic source routing protocol (dsr). In: IETF Internet Draft (2007)

[23] Charles E. Perkins and Pravin Bhagwat. 1994. Highly dynamic Destination-Sequenced DistanceVector routing (DSDV) for mobile computers. In Proceedings of the conference on Communications architectures, protocols and applications (SIGCOMM '94). ACM, New York, NY, USA.

[24] www.tools.ietf.org/html/draft-cole-manetolsrv2- mib-00.

[25] Du, H.; Hassanein, H.; Chihsiang Yeh, "Zonebased routing protocol for high-mobility MANET," Electrical and Computer Engineering, 2003. IEEE CCECE 2003. Canadian Conference on , vol.2, no., pp.1055,1058 vol.2, 4-7 May 2003. [26] Joa-Ng, M.; I-Tai Lu, "A peer-to-peer zonebased two-level link state routing for mobile ad hoc networks," Selected Areas in Communications, IEEE Journal on , vol.17, no.8, pp.1415,1425, Aug 1999.

[27] Yih-Chun Hu; Perrig, A.; Johnson, D.B., "Wormhole attacks in wireless networks," Selected Areas in Communications, IEEE Journal on , vol.24, no.2, pp.370,380, Feb. 2006.
[28] Su, Ming-Yang and Chiang, Kun-Lin," Prevention of Wormhole Attacks in Mobile Ad Hoc Networks by Intrusion Detection Nodes", Wireless Algorithms, Systems, and Applications, Springer Berlin Heidelberg, 2010.
[29] Nait-Abdesselam, F., "Detecting and avoiding wormhole attacks in wireless ad hoc networks," Communications Magazine, IEEE , vol.46, no.4, pp.127,133, April 2008.
[30] Jiwen Cai; Ping Yi; Jialin Chen; Zhiyang Wang; Ning Liu, "An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network," Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on , vol., no., pp.775,780, 20-23 April 2010.

[31] Chen Wei; Long Xiang; Bai Yuebin; Gao Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc Networks," Communications and Networking in China, 2007. CHINACOM '07. Second International Conference on , vol., no., pp.366,370, 22-24 Aug. 2007. [32] Ping Yi; Zhoulin Dai; Yi-ping Zhong; Shiyong Zhang, "Resisting flooding attacks in ad hoc networks," Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on , vol.2, no., pp.657,662 Vol. 2, 4-6 April 2005.
[33] Carl, G.; Kesidis, G.; Brooks, R.R.; Rai, S., "Denial-of-service attack-detection techniques," Internet Computing, IEEE , vol.10, no.1, pp.82,89, Jan.-Feb. 2006.
[34] IEEE standard 802.11–1999, wirless lan medium access control (mac) and physical (phy) specification (1999).