IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Study of Various Security Attacks in Network Layer and the Mitigation Techniques for MANET

R. Divya Paramesvaran[1], Dr. D. Maheswari[2]

Rathnavel Subramainam College of Arts & Science, Coimbatore, Tamil Nadu, India[1, 2]

Abstract: Security is one of the major concerns for protected communication between mobile nodes in a hostile environment. In hostile environments attackers can crew active and passive attacks against intercept able routing in embed in routing message and data packets. In this research, we focus on crucial security attacks in Mobile adhoc networks. MANET has no clear line of deterrence, so, it is accessible to both reasonable network users and malicious attackers. In the existence of malicious nodes, one of the main objections in MANET is to design the robust security solution that can protect MANET from various routing attacks. Yet, these solutions are not suitable for MANET resource constraints, i.e., limited bandwidth and battery power, because they recommend heavy traffic load to exchange and verifying keys. This paper is a study on various security attacks, various mitigation techniques proposed by various Network layers for secure routing and the research on current trends. In particular, we examine routing attacks, as well as remedy against such attacks in existing MANET protocols.

Keywords: Attacks, DSR protocol, MANET, Rushing Attack, Self organization, Router.

I. INTRODUCTION

Wireless communication is growing day by day due to its Increasing applications. In recent years, MANETs (mobile ad-hoc Networks) have received more attention due to its self-creation and self maintenance nature. Each device in MANET is free to move in any direction which results the change in link table frequently. The member nodes are itself responsible for all the link management. Each node in a MANET has its own wireless transmitter and receiver so that nodes can communicate with each other in their wireless range. The nodes which are not within the wireless range communicate with other nodes hop by hop by following some rules known as routing protocols. The latest work is done in wireless technology achieve a lot of attention. An ad-hoc network is one of such advancement in wireless technology which gives a new platform to wireless self organized networks. The ad-hoc networks are not infrastructure networks and create routes when required. They are peer-to-peer network. They are mainly used for military oriented purposes. Confidentiality, integrity, availability, non-repudiation and authentication are the basic requirements of information security [2]. The dynamic nature of mobile ad-hoc networks creates a problem in finding multi-hop routers for communication path. In ad-hoc networks mobile node can move randomly because each node act as a router, so it is very difficult to find an optimal route. Security is still the main topic for many researchers. They provide various security routing protocols for secure communication.

The Authors in [3] presented a design and performance evaluation of new on-demand ad hoc network routing protocol known as Ariadne. Ariadne helps the protocol by preventing attacker from altering with uncompromised routes consisting of such uncompromised nodes. Ariadne also helps to prevent Denial-of-Service attacks. Some more features of Ariadne is that it is efficient and using only efficient symmetric cryptographic operations. They also compared Ariadne to a version of Dynamic source routing (DSR) by disabling all protocol optimizations that are not present in Ariadne and then calculate the effect of optimization and security separately. They prove that Ariadne lowers the packet overhead by 41% than for un optimized DSR. However Ariadne added some cost for security that was not present on unoptimized DSR. Cheng Yong, Huang Chuanhe and Shi Wenming in 2007 suggested novel secure routing protocol for mobile ad-hoc networks known as trusted dynamic source routing (TDSR) [4].

In this a trust score is calculated on the basis of direct trust and indirect trust. When the trust value of the node falls below the threshold then it is added to the blacklist. The nodes that performs below the threshold or present in blacklist are not b forwarded. Dhurandher and Mehra in 2009 [5] introduced the approach that can be used to calculate the trust value of node in a dynamic manner and also protects message modification by attacker. The result is calculated by doing simulations in packet delivery ratio and the number of times packet was broken into parts. By considering behavior of a node a trust value is given to a node. It can be incremented and decremented according to the behavior of node. Trust value can be of three types that are: positive, negative or zero that shows that node is known, malicious or unknown behavior respectively. Pallavi and Trivedi in 2011[6] gave solution to prevent serious attack that is a wormhole attack by the use of digital signatures. In this if a sender wants to send packet to destination node it will create a secure path with the help of digital signature verification. Node sends a packet along with a digital signature and if it matched with the

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

digital signature stored in their database of other nodes then the request is from authentic source. Kamini Nalavade and Dr. B.B. Meshram in June, 2014 gave the layered approach for preprocessing of data in intrusion detection system [7]. To remove unwanted and redundant data from packets, the layered approach of TCP/IP model is used for the faster preprocessing of data in intrusion detection system. S. Saravanakumar, Umamaheshwari, D. Jayalakshmi and R. Sugumar [8] in 2010 handles the issue of complexity and throughput that are the problems in Intrusion Detection System (IDS). The authors compare various IDS systems and then suggest a scheme that uses the combination of artificial neural network algorithms. This combination of algorithm gives better performance. Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU [9] in 2010 proposed the algorithm to detect black hole and gray hole attacks in adhoc networks. The researchers demonstrate the adaptive approach using cross layer design. The authors proved their theory by using path-based method to overhear the next node. So, it saves system resources by not sending out extra control messages. A collision rate reporting system is established to reduce the false positive rate under high network load.

II. SECURITY ATTACKS IN MANET

Mobile Ad hoc networks are vulnerable to various attacks not only from outside but also from within the network itself. Ad hoc network are mainly subjected to two different levels of attacks. The first level of attack occurs on the basic mechanisms of the ad hoc network such as routing. Whereas the second level of attacks tries to damage the security mechanisms employed in the network. The attacks in MANETs are divided into two major types like Internal and External attacks.

Internal Attacks

Internal attacks are directly leads to the attacks on nodes presents in network and links interface between them. This type of attacks may broadcast wrong type of routing information to other nodes. Internal attacks are sometimes more difficult to handle as compare to external attacks, because internal attacks occurs due more trusted nodes. The wrong routing information generated by compromised nodes or malicious nodes are difficult to identify. This can be due to the compromised nodes are able to generate the valid signature using their private keys.

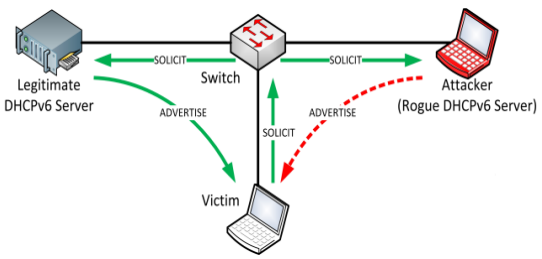

Fig 2.1 Internal attack

External Attacks

External attacks are carried out by nodes that do not belong to the network. It causes congestion sends false routing information or causes unavailability of services. These types of attacks try to cause congestion in the network, denial of services (DoS), and advertising wrong routing information etc. External attacks prevent the network from normal communication and producing additional overhead to the network. External attacks can classify into two categories like active and passive attacks

Passive Attack

A passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

Active Attack

In an active attack, the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. Active attacks are very severe attacks on the network that prevent message flow between the nodes. However active attacks can be internal or external. Active external attacks can be carried out by outside sources that do not belong to the network. Internal attacks are from malicious nodes which are part of the network, internal attacks are more severe and hard to detect than external attacks. These attacks generate unauthorised access to network that helps the attacker to make changes such as modification of packets, DoS, congestion etc. The active attacks are generally launched by compromised nodes or malicious nodes. Malicious nodes change the routing information by advertising itself as having shortest path to the destination.

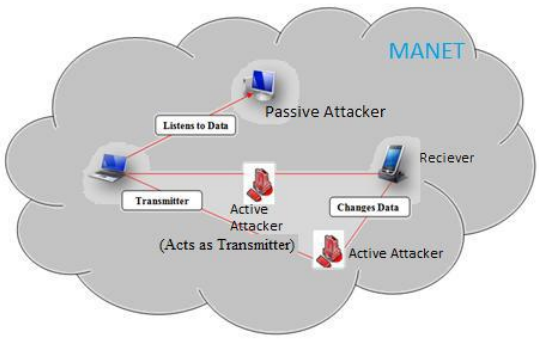

Fig 2.2 Active and Passive Attack in MANET

Active Attacks in Network Layers

Blakehole Attack

In a blackhole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example, in AODV, the attacker can send a fake RREP (including a fake destination sequence

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic.

Figure 2.3 shows an example of a blackhole attack, where attacker A sends a fake RREP to the source node S, claiming that it has a sufficiently fresher route than other nodes. Since the attacker's advertised sequence number is higher than other nodes' sequence numbers, the source node S will choose the route that passes through node A.

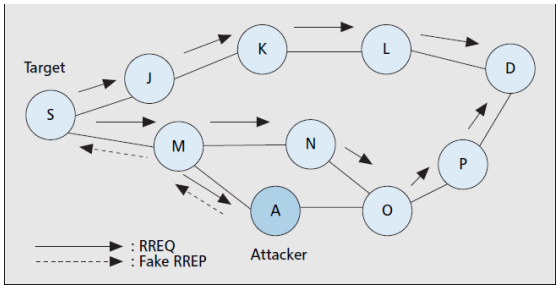

Fig 2.3 Example of Blackhole Attack

Countermeasures for Blackhole Attack

(i) Collecting multiple RREP messages (from more than two nodes) and thus hoping multiple redundant paths to the destination node and then buffering the packets until a safe route is found.

(ii) Maintaining a table in each node with previous sequence number in increasing order.

Each node before forwarding packets increases the sequence number. The sender node broadcasts RREQ to its neighbors and once this RREQ reaches the destination, it replies with a RREP with last packet sequence number. If the intermediate node finds that RREP contains a wrong sequence number, it understands that somewhere something went wrong.

Wormhole Attack

In wormhole attack, malicious node receive data packet at one point in the network and tunnels them to another malicious node. The tunnel exist between two malicious nodes is referred to as a wormhole. Wormhole attacks are severe threats to MANET routing protocols. Attackers use wormholes in the network to make their nodes appear more attractive so that more data is routed through their nodes. When the wormhole attacks are used by attacker in routing protocol such as DSR and AODV, the attack could prevent the discovery of any routes other than through the wormhole. If there is no defence mechanism are introduced in the network along with routing protocols, than existing routing protocols are not suitable to discover valid routes.

For example in fig 2.4, the nodes "X" and "Y" are malicious node that forms the tunnel in network. The source node "S" when initiate the RREQ message to find the route to node "D" destination node. The immediate neighbor node of source node "S", namely "2" and "1" forwards the RREQ message to their respective neighbors "5" and "X". The node "X" when receive the RREQ it immediately share with it "Y" and later it initiate RREQ to its neighbor node "8", through which the RREQ is delivered to the destination node "D". Due to high speed link, it forces the source node to select route <S-1-8-D> for destination. It results in "D" ignores RREQ that arrives at a later time and thus, invalidates the legitimate route <S-2-5- 7-D>.

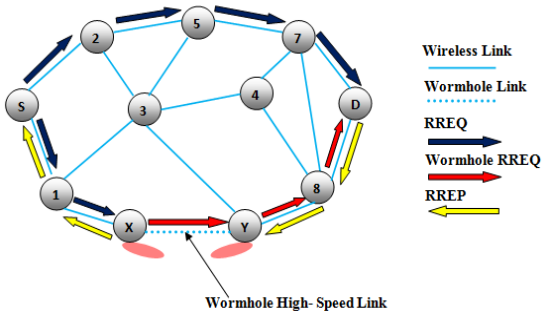

Fig 2.4 Example of Wormhole Attack

Countermeasures for Wormhole Attack

TrueLink is a timing based preventative countermeasure to this attack. Also Packet leashes, are proposed to detect wormhole attack. Leash is any information added to a packet designed to restrict the packet's maximum allowed transmission distance. Geographical leash ensures that the recipient of the packet is within a certain distance from the sender node. Temporal leash ensures that the packet has an upper bound of its lifetime (restricts the maximum travel distance).The SECTOR mechanism is also proposed to detect wormholes without the need of clock synchronization. Directional antennas are also proposed to prevent wormhole attacks.

Rushing Attack

Rushing attacks are mainly against the on demand routing protocols. These types of attacks subvert the route discovery process. On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack . When compromised node receives a route request packet from the source node, it floods the packet quickly throughout the network before other nodes, which also receive the same route request packet can react.

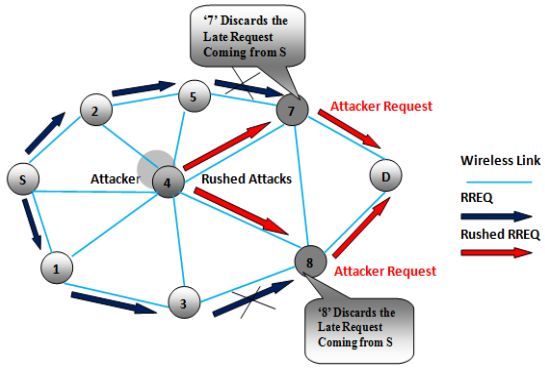

Fig 2.5 Example of Rushing Attack

DOI 10.17148/IJARCCE.2016.5288

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

For example, in figure 2.5 the node "4" represents the rushing attack node, where "S" and "D" refers to source and destination nodes. The rushing attack of compromised node "4" quickly broadcasts the route request messages to ensure that the RREQ message from itself arrive earlier than do those from other nodes. This result in when neighboring node of "D" i.e. "7" and "8" when receive the actual (late) route request from source, they simply discard requests. So in the presence of such attacks "S" fails to discover any useable route or safe route without the involvement of attacker.

Countermeasures for Rushing Attack

SEDYMO: Secured Dynamic MANET On-Demand is similar to DYMO but it dictates intermediate node must add routing information while broadcasting the routing messages and no intermediate node should delete any routing information from previous sender while broadcasting. It also incorporates hash chains and digital signature to protect the identity.

SRDP: Secure Route Discovery Protocol is security enhanced Dynamic Source routing (DSR) protocol.

SND: Secure Neighbor Detection is another method of verifying each neighbor's identity within a maximum transmission range.

Grayhole Attack

Gray Hole attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface. A Gray hole attack is a variation of the black hole attack, where the malicious node is not initially malicious, it turns malicious sometime later. The gray hole attack has two phases. In the first phase, a malicious node exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the node drops the intercepted packets with a certain probability. This attack is more difficult to detect than the black hole attack where the malicious node drops the received data packets with certainly. A gray hole may exhibit its malicious behavior in different ways. It may drop packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of gray hole node may behave maliciously for some time duration by dropping packets but may switch to normal behavior later.

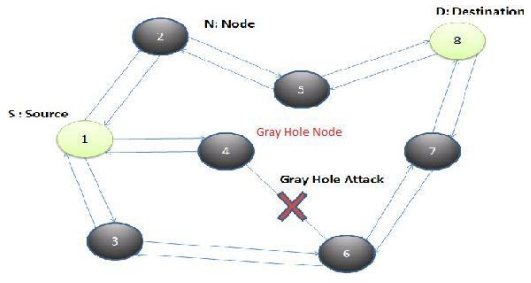

Fig 2.6 Example of Grayhole Attack

Fig 2.6, shows the example of gray hol0e attack on the adhoc network. In this figure node 1 is act as a source node, node 8 act as a destination node. Node 4 represents the gray hole node in above diagram. Node 4 takes the packets from the neighboring node and drops the certain packets during the packet transmission.

Countermeasures for Gray hole Attack

Mitigated by priority protocols schemes. Whenever a node enters in a Mobile Ad Hoc network IP allocation is the first step in which the node will get its IP along with initial priority and we have adopted the technique of Prime DHCP. Neighbor Discovery is the second step of the proposed scheme. New node will send the HELLO packets to its neighbors and discover the identity of the neighbors along with their priority. Authentication is the next step of the scheme in which it will broadcast information about its existence and exchange keys with the neighbors according to the scheme HEAP which is a hopby- hop authentication protocol. HEAP authenticates packets at every hop by using a modified HMAC based algorithm along with two keys and drops any packets that originate from outsides.

Sybil Attack

In Sybil attack, Sybil attacker may generate fake identities of number of additional nodes. In this, a malicious node produces itself as a large number of instead of single node. The additional identities that the node acquires are called Sybil nodes. A Sybil node may fabricate a new identity for itself or it steals an identity of the legitimate node. A faulty node or an adversary may present multiple identities to a network in order to appear and function as multiple distinct nodes. After becoming part of the network, the adversary may then overhear communications or act maliciously. By presenting multiple identities, the adversary can control the network substantially.

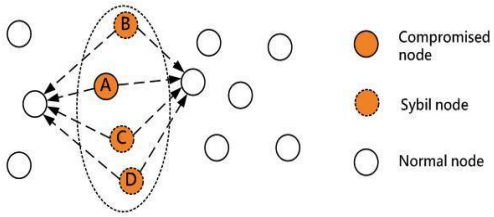

Fig 2.7 Example of Sybil Attack

Countermeasures for Sybil Attack

One way of mitigating this attack is maintaining a chain of trust, so single identity is generated by a hierarchical structure which may be hard to fake. Another approach would be based on signal strength. A robust Sybil attack detection framework is proposed for MANETs based on cooperative monitoring of network activities.

Validation techniques can be used to prevent Sybil attacks and dismiss masquerading hostile entities. A local entity may accept a remote identity based on a central authority which ensures a one-to-one correspondence between an identity and an entity and may even provide a reverse lookup. An identity may be validated either directly or indirectly. In direct validation the local entity queries the central authority to validate the remote identities. In indirect validation the local entity relies on already accepted identities which in turn vouch for the validity of the remote identity in question.

DOI 10.17148/IJARCCE.2016.5288

Identity-based validation techniques generally provide accountability at the expense of anonymity, which can be an undesirable tradeoff especially in online forums that wish to permit censorship-free information exchange and open discussion of sensitive topics. A validation authority can attempt to preserve users' anonymity by refusing to perform reverse lookups, but this approach makes the validation authority a prime target for attack. Alternatively, the authority can use some mechanism other than knowledge of a user's real identity - such as verification of an unidentified person's physical presence at a particular place and time - to enforce a one-to-one correspondence between online identities and real-world users.

3. CONCLUSION

Mobile ad-hoc network has been active research based area over the past few years, due to their application in military and civilian communication. But it is vulnerable to various types of attacks. Misconduct of nodes causes the damage to the nodes & packet also. This paper gave all the stock information about the security of ad hoc networks. In the introduction section we discussed about the MANETs, routing protocols and its types. In the next part, we discussed some of the main security attacks that are vulnerable to ad hoc networks. This paper proposed the related work on the security threat by many researchers and the research gap in this field. Lot of work is going on the security attacks by intruder. This paper is a survey on various methods that are proposed by researchers to prevent security attacks and the researchers should more focus about security of MANETs.

REFERENCES

[1] Jayraj Singh, Arunesh Singh, Raj Shree "An Assessment of Frequently Adopted Security Patterns in Mobile Ad hoc.
[2] Stallings W [2000], Network Security Essentials: Security Attacks. Prentice Hall. (pp. 2-17).
[3] YIH-CHUN HU□and ADRIAN PERRIG Carnegie Mellon University, USA DAVID B. JOHNSONRice University, USA.in 2005.
[4] CHENG Yong, HUANG Chuanhe, SHI Wenming, "Trusted Dynamic Source Routing Protocol", Wireless Communications, International Conference on Networking and Mobile Computing, WiCom2007, Sept. 21-25,2007,pp.1632-1636.
[5] Sanjay K. Dhurandher, Vijeta Mehra, "Multi-path and Message Trust-Based Secure Routing in Ad Hoc Networks", International Conference on Advances in Computing, Control, and Telecommunication Technologies, ACT '09. Dec. 28- 29, 2009, pp.189-194.
[6] Pallavi Sharma, Aditya Trivedi, "An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature", 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN), May 27-29 2011, pp.307-311.
[7] International Journal of Computer Applications Technology and Research (IJCATR) Volume 3 Issue 6 June 2014 Layered Approach for Preprocessing of Data in Intrusion Prevention Systems Kamini Nalavade, Dr. B. B. Meshram.
[8] S. Saravanakumar, Umamaheshwari, D. Jayalakshmi, R. Sugumar, "Development and implementation of artificial neural networks for intrusion detection in computer network", Int. Journal of Computer Science and Network Security2010. vol. 10, no. 7, pp. 271-275.
[9] Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU, "An Adaptive Approach to Detecting Black and GrayHole Attacks in Ad Hoc Network", 2010 24th IEEE International Conference on Advanced Information Networking and Applications (AINA),Perth, Australia, April 20-23, 2010, pp.775-780.
[10] D.Sheela, Naveen Kumar. C, G.Mahadevan, "A Non-Cryptographic method of Sink HoleAttack Detection in Wireless Sensor Networks", 2011 International Conference on Recent Trends in information Technology(ICRTIT),Chennai, India, June 3-5, 2011, pp.527-532.
[11] Quan Jia, Kun Sun, Angelos Stavrou, "CapMan: Capability based Defense against Multi-Path Denial of Service (DoS) Attacks in MANET", Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN), Maui, HI, USA 2011, July 31-August 4, 2011, pp.1-6.
[12] Japing Wang, Haoshan Shi, "A Secure DSR Protocol Based on the Request Sequence-Number", 5th International Conference on Wireless Communications, Networking and Mobile Computing, 2009 (WiCom '09), Beijing, China, Sept. 24-26, 2009, pp. 1-4.
[13] Muhammad Zeshan, Shoab A. Khan, Ahmad Raza Cheema, Attique Ahmed, "Adding Security against Packet Dropping Attack in Mobile Ad hoc Networks", International Seminar on Future Information Technology and Management Engineering, (FITME '08), Leicestershire, UK, Nov. 20. 2008, pp.568-572.
[14] Gunhee Lee, Dong-kyoo Kim, Jungtaek Seo, "An Approach to Mitigate Wormhole Attack in Wireless Ad Hoc Networks", International Conference on Information Security and Assurance (ISA 2008), April 24-26, 2008, pp.220-225.
[15] Thanachai Thumthawatworn, Tapanan Yeophantong, Punthep Sirikriengkrai, "Adaptive Sinkhole Detection on Wireless Ad Hoc Networks", Proceedings of IEEE Aerospace Conference, 2006,Big Sky, Montana, USA, 4-11 March 2006,pp.1-10.
[16] Benjamin J. Culpepper, H. Chris Tseng, "Sinkhole Intrusion Indicators in DSR MANETs", Proceedings of First International Conference on Broadband Networks (BroadNets 2004),San Jose, USA, Oct. 25-29, 2004, pp. 681- 688.
[17] Jaydip sen et. al "A Mechanism for Detection of Gray Hole Attack in Mobile AD Hoc Networks" ICICS 2007, IEEE.
[18] H. Hallani, S.A. Shahrestani, "Trust Assessment in Wireless Ad-hoc Networks", Wireless Days, 2008 (WD '08). 1st IFIP, Dubai, Nov. 24-27, 2008, pp.1-5.