ISSN:2320-0790

An International Journal of Advanced Computer Technology

Attacks analysis and countermeasures in routing protocols of mobile ad hoc networks

Dr Karim KONATE, GAYE Abdourahime

Department of Mathematics and Computing
University Cheikh Anta DIOP Dakar, Senegal

Abstract: The present work is dedicated to study attacks and countermeasures in MANET. After a short introduction to what MANETs are and network security we present a survey of various attacks in MANETs pertaining to fail routing protocols. We also present the different tools used by these attacks and the mechanisms used by the secured routing protocols to counter them. Our work ends with a table which summarizes the advantages and the disadvantages of the mechanisms proposed were presented.

Keywords: Mobile Ad Hoc; routing; security; attacks; countermeasure

I. INTRODUCTION

We have witnessed an exponential deployment of the spontaneous networks thanks to the emergence of new technologies wireless and, and also to the increasing availability of advanced and autonomous terminals (telephones, PDAs). An Ad hoc network constitutes a regrouping of a large population of portable calculating units (laptops, PDA) inter-connected by a wireless technology, moving in an unspecified territory, forming a decentralized network, without fixed infrastructure.

This network is usually characterized by a dynamic topology, a limited bandwidth, energy constraints, the heterogeneity nodes, and a limited physical security. The applications having recourse to the ad hoc networks cover a very broad spectrum. For example in the tactical applications (fires, flood, etc.), in the soldier's field, in the monitoring systems, and the world of transport [1].

The problem of the MANET is how to find the investment of lower costs in rated capacities and reserves which ensures the routing of the nominal traffic and guarantees its reliability in the event of any breakdown of arc or node. That's why several families routing protocols emerged. Each protocol can be classified as a reactive like AODV (Ad hoc One Demand Distance Vector) and DSR (Dynamic Source Routing), proactive like OLSR (Optimized Link State Protocol), or hybrid like ZRP (or Routing Protocol Zones) [1].

In spite of the evolution of the ad hoc mobile networks during the last decade it still problems related security which remain unsolved. Although some solutions were proposed none of them can't satisfy all the constraints on the ad hoc networks.

II. ATTACKS ANALYSIS AND COUNTERMEASURE IN ROUTING PROTOCOL OF MOBILE AD HOC NETWORKS

An attack is an action which aims at compromising the security of the network. The attacks of security can be classified in two categories according to nature of the attacker: Passive Attacks: the attacker can only listen clandestinely or monitor the traffic of the network. Typically it is the easiest form of the attack and it can be accomplish without difficulty in many environments of network management, for example the emission networks such as Ethernet and the wired networks. In the case of the active attacks, the attacker can not only listen the transmission but can also actively change it or block it. They are many and varied in these MANET.

Blackhole attack: consists in dropping some routing messages that node receives [01, 02, 03, 04, 05]. It was declined in several particularity alternatives, having different objectives, among which we can quote:

- Routing loop, which makes it possible for a node to create loops in the network;
- Grayhole, which lets pass only the packages of routing and diverts the data;
- Blackmail, which makes it possible for a node attacker to isolate another node.

Several solutions exist to counter these types of attacks, among which we name the technical estimate relation. In

this mechanism the authors classified the relation between the nodes and their neighbours in three cases: Unknown (node X sent forever (received) of messages to (from) the node y and the probability of the malevolent behaviour are very high), acquaintance (node X sent (received) some messages to (from) the node y and the probability of the malevolent behaviour must be observed) and Friend (node X sent (received) in abundance of the messages to (from) the node y and the probability of the malevolent behaviour is too small. This mechanism is implemented in the routing protocol RDSR (Relationship enhanced DSR protocol) [06].

The Threshold of sequence number consists in performing a check to find if RREP seq no is higher than the threshold value. The threshold value is dynamically updated in each interval of time. As the value of RREP seq no proves higher than the threshold value, one suspects the node to be malicious and adds it to the black list. This mechanism is implemented in the routing protocol DPRAODV (Detection, Prevention and Reactive AODV) [21].

The Watchdog or monitoring (watchdog) is a solution which makes it possible to identify malicious nodes. The Watchdog assigns positive values with a node which successfully forwarded packages and a negative value after a threshold level of bad behaviour was observed. It's implemented in SWAN (mobile Secure Watchdog for Ad hoc Network) [14]. Pathrater which makes it possible the protocol to avoid nodes corrupted register in a black list [14].

The DRI or the data table of information's routing which is used to identify nodes of cooperative blackhole, it consists in adding two additional bits of information. These bits have as values 0 for "FALSE" and 1 for" TRUE " for intermediate nodes answering the RREQ of node source, AODV implements this mechanism [22,23]. The Cross checking solution which consists in hoping on reliable node (nodes by which node source has forwarded the data) to transfer from the packets of data [22, 23].

Wormhole attack: this consists in putting a tunnel between two malicious nodes, often two attackers [01, 03]. To fend off the Wormhole attacks some authors proposed to use the concept of Hop-count Analysis. In this mechanism, a route which has a low or high hop counted is considered to be nonusable. A so low hop counted can imply an attack of wormhole; while a high hop can also slow down the transmission. The protocol Multipath Hop-count Analysis (MHA) implements this mechanism and also protocol AODVWADR (AODV Wormhole Attack Detection Reaction) [12, 13].The clustering consists in dividing the network clusters with for each one a head and members. When a node in the ith cluster suspects an attack wormhole of the layer 1 in the cluster, it informs the head of the ith cluster. The heads of the clusters of the layer1 inform its members respectively. This mechanism is implemented in the protocol in AODV [14]. The packet leash which can be geographical which ensures that the recipient of the packet is in at certain distance from the sender or temporal who ensures that the packet has a superior i.e. sender node which deals the time to live. The protocols LAR (Location Aided Routing) and AODVWADR (AODV Wormhole Attack Detection Reaction) implement this mechanism [01, 11] and also the directional antennas (Directional antenna) which consists in using the direction of the packets of arrival to detect if the packets come from their own neighbors. This solution is implemented in DREAM (Distance Routing Effect Algorithm for Mobility [15].

Rushing attack: this consists in much rather sending requests for routes (RREQs) to the receiver than faster, than other requests routes coming from other intermediate nodes. There is a probability of forcing the routes to pass by him [01, 03]. To solve these types of attacks some solutions were proposed among which we can randomly quote the concept of selection (randomized selection) which consists in admitting a random selection of the messages of route request. Thus a node waits until collecting a threshold number of route requests. According to this number of collected requests, the node can randomly choose a request to transfer among the received requests. The authors proposed to implement it under DSR [11]. There is also the Detection of sure neighbour (Secure Neighbour Detection) who allows each node to check that the other neighbour is with the maximum range of transmission. It is carried out by the observation of the challenge response delay to evaluate the distance to a node and to check if the node can be a neighbour. In other it exists solution called delegation of route sure (Secure road Delegation) which makes it possible each node to check that all the stages of detection of vicinity were carried out between any pair of adjacent nodes, i.e. to check that nodes are indeed neighbours. A delegation route message is exchanged (Route Delegation / Accept). This mechanism is implemented in RAP (Rushing Attack Prevention) [11].

The selfish attack: consists in not collaborating for the good performance of the network. We can identify two types of nodes which do not wish to take part in the network. Defective nodes i.e. do not work perfectly. Those which are malevolent, it is those which intentionally, try to tackle the system: attack on the integrity of the data, the availability of the services, the authenticity of the entities (denial-of-service, interception of messages, usurpation of identity, etc). Selfish nodes are entities economically rational whose objective is to maximize their benefit. To prevent the selfish nodes some solutions were proposed. Among these we have a solution based on the Negative Selection Algorithm (NSA). It's based on the principles of the discrimination of self or no self in the immune system (to define it to oneself like a collection S of elements in a characteristic space X, a collection which needs to be supervised) [21]. The detection of anomaly aims at distinguishing a new model like part of self or no-self, given a model of system of self [21]. Structured GA (SGA) is a type of evolutionary algorithm which incorporates the redundant genetic material, which is controlled by a mechanism of gene activation. It uses the multi-layer

genomic structures for its chromosome i.e. all the genetic material (expressed or not) is structured in a hierarchical chromosome. The activation and deactivates mechanism these coded genes. This solution is implemented in AODV [21].
A solution based on the reputation (CORE and CONFIDANT) which consists in collecting information on an old behaviour of the tested entity by others [08, 09, 10].
A solution based on the payment (Nuglet) which requires with nodes which benefit from the resources of the network (transmitters and/or receivers) to pay" service providers" (intermediate nodes) [09, 10] and a solution based on the localization (directional antennas).

Sleep deprivation: consists to make a node to remain in a state of activity and to make him consume all its energy [04]. To fend off the sleep deprivation we have recourse to some solutions. One which is based on the selection of advised energy and which takes into account the energetic considerations in the choice of the best route. Each node calculates its own energetic statute and declares an appropriate prediction. The choice of the prediction is based over the capacity of the battery and the lifetime envisaged of a node. The relationship between real and initial energy of a node is used to measure the capacity of battery. This mechanism is implemented in protocol EEAOMDV: Energy Efficient Ad hoc One Demand Multipath Outdistances Vector Routing Protocol [22].
One which is based on the effective Energy for the routing; it requires a dynamic commutation on the states of the nodes between the sleep mode and the active mode. The nodes enter these states with fixed intervals in order to ensure the forwarding of the messages successfully; the active nodes can retransmit messages some times before the node of destination is in listening or activity. This mechanism is implemented in BECA: BASIC Energy Conserving Algorithm [23].
One which is based on PARO (control of power of the routing) which is a technique of control power routing for MANETs where all nodes are located in the maximum range transmission of the one another i.e. energy depends on the distance which separates the source and the destination [24]. The solution which is based on PAA (Alternation of the control power) consists in eliminating the network activity for a group of nodes during some period in order to preserve their energy and to keep their presence in the network by a delegation [25].

Location disclosure attack: consists in revealing information on the position of intermediate nodes or the structure's network [26]. To prevent the attacks of location disclosure the algorithm named RNI: Random Node Identification is proposed. It is based on the use for a random identify of node to dissociate true identifying node of the information's site. The authors proposed to implement the solution of the RNI in protocol AODV (Ad hoc One-demand Outdistances Vector) [04].
Overflow routing tables: consists of malicious nodes to cause the overflow routing tables of nodes being used as relay [04]. To fend off this attack the named solution Trust evaluation was proposed. It's based on the evaluation of confidence to ensure a secure routing in MANETs. The success of a communication through a node will increase the index of confidence of this node and the failure by this node will decrease the index of confidence. If this value reaches zero this node is registered in a blacklist and we inform the other neighbors. TRP (Trust-based Routing Protocol) implements this solution [20].

Ad hoc flooding attack: This makes it possible for an adversary to carry out DoS by saturating the support with a quantity of broadcasting messages, by reducing the output of nodes, and in the worst case, to prevent them from communicating [28]. To prevent saturation on the level of nodes two principal approaches were proposed. An approach based on the Relationship, in this mechanism, all the nodes in an ad hoc network are classified by categories: friends, knowledge or foreigners, based on their relationship with their neighbour nodes. During the initialization of the network all the nodes will be foreigners between them. A confidence estimator is used in each node to evaluate the degree of confidence of his neighbours. This solution is implemented in protocol AODV) [29].
An approach based on the virtual currency which uses the concept of credit or micro payment to compensate for the node service [20]. An approach based on the method of neighbour suppression (FAP). When the attacker diffuses a large number of RREQ packets, the neighbour nodes to the attacker record the rate of requests for routes. Once the threshold is exceeded, the neighbour nodes deny all the future packets of request of the attacker.

Replay attack: which consists in propagating the old routing messages, which do not reflect current topology, in the network to affect routes? To prevent this attack type the mechanism of Sequence Number was proposed and they make it possible for distinction between the old and the new transmitted packets. DSDV (Dynamic Destination Sequence Distance Vector) and AODV (Ad hoc On demand Distance Vector) implement the mechanism [01].

They are many attacks and the protocols which implement these above mentioned mechanisms do not resist with these types of attacks. The following table recapitulates the advantages and the disadvantages of the countermeasures proposed to fend off the attacks in the routing protocols of MANET.

Table 1: table recapitulates the advantages and the disadvantages of the protocols

Attacks and protocols				
Attacks	**Mechanisms**	**Protocols**	**Advantages**	**disadvantages**
Blackhole attack	**Relationship enhanced**	**RDSR (Relationship enhanced DSR protocol)**	allows to build trust paths	- flooding of the bandwidth owned to send a large quantity of messages to increase its trust degree - The paths of the legitimate nodes recently come will be get round.
	Threshold of sequence numb er	**DPRAODV: Detection, Prevention and Reactive AODV**	- Isolated a malicious node grace to the control packages. - Reduction of the routing load owned to the blocking replays of the malicious nodes.	A malicious node can deliberately send a control package to isolate a legitimate node
	Watchdog	**SWAN : Secure Watchdog for mobile Ad hoc Network**	Encourage the forwarding of the messages even if they are malicious to avoid the black list.	- Bad behavior accused by a malicious node. - Two malicious nodes can cooperate - problem of storage
	Pathrater			
	Data routing information table	**AODV : Ad hoc On-demand Distance Vector**	force the malicious nodes to have a good behavior for forwarding the routing packages not to be consider as unreliable	the malicious node can make the routing correctly and divert the packages of data
	Cross checking			
Wormhole attack	**Hop-count Analysis**	**MHA: Multipath Hop-count Analysis** **AODV-WADR : AODV-Wormhole Attack Detection Reaction**	reduce to the minimum the utilization rate of wormhole route	Possibility of choosing a route which contains an attacker creating a blackhole attack.
	clustering	**AODV**	Force the wormhole nodes to forward the messages in order to haven't a Δp which overcomes the threshold value defined by the monitoring node	- a loss of energy owned to the continuous monitoring network - Consumption of the memory and CPU resources owned to the many calculations make for the control packages. - total dysfunction of the network in case of attack or breakdown of the guard node or the head cluster node
	Leash geographical	**LAR : Location-Aided Routing**	- reduce the maximum distance that the package is authorized to cross in order to be able to reject certain packages	- To have synchronous clocks.
	Leash temporal			
	Directional enteena	**DREAM: Distance Routing Effect Algorithm for Mobility**	- to evaluate the neighbors declarations - It uses energy efficiently - reduce the collisions	- when there are also obstacles the calculation of the distance could still generate Wormhole
Rushing attack	**randomized selection**	**Proposed To implementation in DSR**	- choose the good route request	- choose the request of malicious node - capacity of storage - consumption of energy
	Secure Neighbor Detection	**RAP : Rushing Attack Prevention**	- know the neighbors - detect the false declarations	- distinction between the corrupt nodes and the others - occupation of bandwidth
	Secure route Delegation			
The selfish attack	**Negative Selection Algorithm**	**AODV**	- allow the detection of the change network -favoured the collaboration of the nodes by the detection of genes	- a waste of energy owned to the continuous monitoring - dysfunction of the network in case of attack or breakdown of the genetic node
	Anomaly Detection			
	structured GA			
	Watchdog	**CORE**	- force the node to have well behaviors with the future in order not to lose their reputation - encourage the nodes to cooperate - forwarding the packages by the malicious nodes	- distinction between the useful packages - Two malicious nodes can cooperate - frequent detection in CONFIDANT
	Reputation	**CONFIDANT**		
	Virtual Currency	**Nuglets**	- discourage sending useless messages - to off-load the network - availability of bandwidth	- The source should overestimate the number of nuglets. - The intermediate nodes can deny the forwarding service - require to have an authority which charges to the updating
	Directional enteena	**LAR : Location-Aided Routing**	- to assess the declarations of neighbors - It uses energy efficiently -reduce the collisions	when there are also obstacles the power of the antennas will be able to decrease causing an attenuation of the signal
Sleep Deprivation	**Energy Efficient**	**EEAOMDV: Energy Efficient Ad Hoc On Demand Multipath Distance Vector Routing Protocol**	- allowed to choose the best routes - - to balance the consumption of nodal energy	- Declaration of low prediction in order to preserve its energy for its own use. - declaration of high prediction to be considered as reliable causing an attack blackhole
	Energy-Conserving	**BECA : Basic Energy-Conserving Algorithm**	- allows the nodes which have a limited autonomy of energy to gain more energy	- Sending messages to a legitimate node leading to an enormous consumption of energy. - The retransmission of the messages engenders a saturation of the bandwidth - An overload of the network.
	Power Aware Routing	**PARO : Power Aware Routing**	- allows the nodes which have a limited autonomy of energy to gain more energy - make a choice of sure neighbors.	- an elected node can be attacked by a malicious node - overload of network - reduce the available bandwidth
	Alternation of the inactivity and working periods with the supporteurs	**PAA : Power Aware Alternation**	- save on energy - reduce the interferences - reduction of the loss packages owed the size of the network.	- limited capacity of storage - a malicious node can also send REJECT messages - waste of energy
Localison disclosure attack	**RNI : Random Node Identification**	**Proposed to modify AODV : Ad hoc On-demand Distance Vector**	A malicious node cannot show the change of RNI node	-identifier collision - waste of energy owed the processing time
Overflow	**Trust evaluation**	**TRP : Trust-based Routing Protocol**	- isolate the malicious nodes - eliminate the fictitious declaration route	- the potentially malicious nodes which did not have knowledge on the other nodes, with time they will know each other more and more - the node which has been just connected cannot profit from this trust
Ad hoc flooding attack	**Relationship**	**AODV**	- Prevent the flooding of RREQ to indicate the threshold values - favoured the cooperation of malicious nodes	- distinction between the rite and the wrong messages - a high probability of new nodes to be consider as attackers
	Virtual currency	**Nuglets**	-discourage the sending useless message - off-load the network - availability of bandwidth	- a malicious node usurp the address of legitimate node in order to be considered as legitimate - the node of the network periphery will have less chance to be rewarded
	suppression neighbour	**FAP : Flooding Attack Prevention**	- do not flooding the network of messages - availability of network increasing the bandwidth	- problem of storage - problem of time owed the consultation of tables

The following table recapitulates the protocols and the attacks which the protocols can counter

Table 2: table recapitulates the protocols and the attacks

Routing protocols / Attacks	SWAN	LAR	RAP	CORE	CONFIDANT	Nuglet	PARO	PAA	TRP	FAP	DSDV	AODV	WRP	DREAM	RDSR	DPRAODV	MHA
Routing loup	yes	no	yes	yes	yes	no	no	no	yes	no	yes	yes	yes	yes	yes	yes	no
Grayhole	yes	no	no	yes	yes	no	no	no	yes	no	no	no	yes	yes	yes	yes	no
Blackmail	yes	no	yes	no	no	no	no	no	no	no	no	no	no	no	yes	no	no
Wormhole	no	yes	yes	no	no	no	yes	no	no	no	no	yes	yes	yes	no	no	yes
Rushing	no	no	yes	no	no	yes	no	no	no	no	no	no	no	no	no	no	yes
selfish	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	no	no	yes	yes	no	no
sleep depivation	no	no	no	no	no	yes	yes	yes	no	yes	no	no	no	no	no	no	no
Location disclosure	yes	no	no	no	no	no	no	yes	no	no	no	no	no	no	no	no	no
Overflow	no	no	yes	no	no	yes	yes	no	yes	no	no	no	no	no	no	no	no
BlackHole coopérative	no	no	no	no	no	no	no	no	no	no	no	no	yes	yes	no	no	no
Ad hoc flooding	no	yes	no	no	no	yes	no	yes	no	yes	no	no	no	no	no	yes	no
Replay	no	no	no	no	no	no	no	no	no	no	yes	yes	no	no	no	no	no

III. DISCUSSION

The world needs more and more mobility, the access and the sharing of information. This mobility materializes by the miniaturization of the peripherals (PDA, digital camera, mobile phone.). This equipment is characterized by modest computing capacities and storage and also their energy autonomy etc. In the ad hoc networks the intermediate nodes are of use bridges or relay for the other mobile nodes of the network. The routing problem in the ad hoc networks is the most difficult challenge to realize, because it is to find the optimal multi-hops route which connects two any nodes of the network. This routing is thus a problem of optimization under constraints of which we can quote the changes of topologies and the volatility of the links, the limited capacity bandwidth, the batteries level energy, etc. However, it arises a problem of adaptation, routing methods of the data i.e. the routing necessary to forward the packets from a point to another point of the network, which is due to the miniaturization and the mobility of the equipment that composes these networks. This routing protocols adaptation used with a great number of existing units in an environment characterized by modest computing capacities and backup creates security holes. It's very important in the future to propose analytical models and simulation cases to see the impact of the attacks

IV. CONCLUSION

To resulting from our work we had specificities of the ad hoc mobile networks, the problems of security of routing protocols in these networks. We presented several alternatives of attacks met in MANETs, their operating process thus the mechanisms used and the protocols which implement them to counter these attacks. The advantages and the disadvantages of all these mechanisms recapitulated in the table.

V. REFERENCES

[1] Wiley John: SEURITY for WIRELESS AD HOC NETWORKS. Eyrolles, book 2007, pages 247.

[2] ADJIDO Idjiwa, BENAMARA Radhouane, BENZIMRA Rebecca, GIRAUD Laurent: secure Protocol routing of ad hoc in a clusterized architecture. University Pierre and Marie (Paris VI) Paris, FRANCE, November 2005, pages 4.

[3] Curtmola Reza. Security of Routing Protocols in Ad Hoc Wireless Networks. 600.647 Advanced Topics in Wireless Networks, February 2007, pages 26.

[4] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei. A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks. Department of Computer Science and Engineering Florida Atlantic University, December 2005

[5] Chen Ruiliang, Snow Michael, Park Jung-Min, M. Refaei Tamer, Eltoweissy Mohamed. Defense against Routing Disruption Denial-of-Service Attacks in Mobile Ad Hoc Networks. Department of Electrical and Computer Engineering Virginia Polytechnic Institute and State University Blacksburg, VA, USA, November 2005, pages 15.

[6] A.Rajaram, Dr. S. Palaniswami. The Trust-Based MAC-Layer Security Protocol for Mobile Ad hoc Networks.. (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 02, 2010, 400-408. Anna University Coimbatore, India, March 2010, pages 9.

[7] Payal N. Raj, Prashant B. Swadas. DPRAODV: A DYANAMIC LEARNING SYSTEM AGAINST BLACKHOLE ATTACK IN AODV BASED MANET, IJCSI International Journal of Computer Science Issues, Vol. 2, Computer Engineering Department, SVMIT Bharuch, Gujarat, India, September 2009, pages 6.

[8] Xue Xiaoyun. Security mechanisms for ad hoc routing protocols. Computer Science and Network Department, ENST, thesis September 2006, pages 234.

[9] Ramaswamy Sanjay, Fu Huirong, Sreekantaradhya Manohar, Dixon John and Nygard Kendall: Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks. Department of Computer Science, IACC 258 North Dakota State University, Fargo, ND 58105, March 2003, pages 7.

[10] Hesiri Weerasinghe and Huirong Fu. Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation ; International Journal of Software Engineering and Its Application Vol. 2, No. 3. Oakland University Rochester MI 48309 USA, June 2008; page 16.

[11] Hu Yih-Chun, Perrig Adrian, Johnson David B.: Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks, INFOCOM 2003, pages 11

[12] Emmanouil A. Panaousis, Levon Nazaryan, Christos Politis. Securing AODV Against Wormhole Attacks in Emergency MANET Multimedia Communications, Wireless Multimedia and Networking (WMN) Research Group Kingston University London. Jully 2009, pages 7.

[13] Shang-Ming Jen 1, Chi-Sung Laih 1 and Wen-Chung Kuo. A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET.

[14] Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki. A NEW CLUSTER BASED WORMHOLE INTRUSION DETECTION ALGORITHM FOR MOBILE AD HOC NETWORKS. International Journal of Network Security and Its Applications (IJNSA), Vol 1, No 1, West Bengal University of Technology, Kolkata 700064, India. April 2009, pages 9.

[15] Hu Lingxuan et Evans David: Using Directional Antennas to Prevent Wormhole Attacks. University of Virginia, California, USA. February 2004, pages 11.

[16] T.V.P.Sundararajan and Dr.A.Shanmugam. Behavior Based Anomaly Detection Technique to Mitigate the Routing Misbehavior in MANET. Sathyamangalm 638401, Tamilnadu,, India, May 2009, pages 14.

[17] Kevin Ho man, David Zage, and Cristina Nita-Rotaru. A Survey of Attack and Defense Techniques for Reputation Systems. Department of Computer Science and CERIAS, Purdue University. April 2008, pages 19.

[18] Pietro Michiardi: Cooperation in the ad hoc networks: Application of the evolution and game theory and the evolution of imperfect observability. Institute Eurecom 2229, road of the Peaks LP 19306904 Sophia-Antipolis, France, July 2006, pages 17

[19] Michiardi Pietro and Molva Refik: CORE: A Collaborative Reputation Mechanism to enforce node cooperation in

Mobile Ad hoc Networks. European Wireless Conference, Nonvember 2003, pages 15.

[20] Hu Jiangyi: Cooperation in Mobile Ad Hoc Networks. Computer Science Department Florida State University, January 11, 2005, pages 23.

[21] Buttyan Levente and Hubaux Jean-Pierre: Nuglets: a virtual Currency to Stimule Cooperation in Self-Organized Mobile Ad Hoc Networks. Institute for Computer Communications and Applications Department of Communication Systems Swiss Federal Institute of Technology Lausanne, 18 January 2001, pages 15.

[22] GETSY S SARA, NEELAVATHY PARI.S, SRIDHARAN.D. Energy Efficient Ad Hoc On Demand Multipath Distance Vector Routing Protocol, International Journal of Recent Trends in Engineering, Vol 2, No. 3. Department of Electronics and Communication Engineering, CEG Campus, Anna University Chennai, India November 2009, pages 3.

[23] Mads Dar Kristensen and Niels Olof Bouvin. Energy E cient MANET Routing Using a Combination of Span and BECA/AFECA. JOURNAL OF NETWORKS, VOL. 3, NO. 3, New York, USA, MARCH 2008, pages 8.

[24] S ARVIND, DR.T.ADILAKSHMI. POWER AWARE ROUTING FOR MOBILE AGENT IN AD-HOC NETWORKS. Journal of Theoretical and Applied Information Technology. Department of Computer Science Engineering, Vasavi College of Engineering, Hyderabad-500031. Mai 2009, pages 7.

[25] Idoudi Hanen, Akkari Wafa, Belghith Abdelfatteh, Molnar Miklos: Synchronous alternation for the conservation of energy in the ad hoc mobile networks. MADE IRIDESCENT, University Center of Beaulieu-35042 Rennes Cedex-France, November 2006, pages 46.

[26] Choi Heesook, McDaniel Patrick, La Porta Thomas F.: Privacy Preserving Communication in MANETs. Department of Computer Science and Engineering the Pennsylvania State University, March 2007, pages 10.

[27] Yan Zheng, Zhang Peng, Virtanen Teemupekka. Trust Evaluation Based Security Solution in Ad Hoc Networks. Helsinki University of Technology, Finland, December 2003, pages 14.

[28] Yi Ping, Dai Zhoulin, Zhang Shiyong, Zhong Yiping: A New Routing Attack in Mobile Ad Hoc Network. Department of Computing and Information Technology, Fudan University, Shanghai, 200433, China, June 2005, pages 12.

[29] Revathi Venkataraman, M. Pushpalatha, and T. Rama Rao. Performance Analysis of Flooding Attack Prevention Algorithm in MANETs. World Academy of Science, Engineering and Technology 56, September 2009, pages 4.

[30] Aad Imad, Hubaux Jean-Pierre, Knightly Edward W. Impact of Denial of Service,Attacks on Ad Hoc Networks. DoCoMo Euro-Labs EPFL Rice University Munich, Germany Lausanne, Switzerland Houston, TX, July 2007, pages 14.

[31] Aad Imad, Hubaux Jean-Pierre, Knightly Edward W. Denial of Service Resilience in Ad Hoc Networks; MobiCom'04, Sept. 26Oct. 1, 2004, Philadelphia, Pennsylvania, USA, pages 14.