WELL-ORGANIZED AD-HOC ROUTING PROTOCOL BASED ON COLLABORATIVE TRUST-BASED SECURE ROUTING

Abdalrazak T. Rahem[1], H K Sawant[2]
[1,2]Department of Information Technology, Bharati Vidyapeeth Deemed University
College of Engineering, Pune-46, India
abdtareq@gmail.com

ABSTRACT

Communication privacy is becoming an essential security requirement for mission critical communications and communication infrastructure protection. Wireless networking is an emerging technology that allows users to access information and services electronically, regardless of their geographic position. The use of wireless communication between mobile users has become increasingly popular due to recent performance advancements in computer and wireless technologies. This has led to lower prices and higher data rates, which are the two main reasons why mobile computing is expected to see increasingly widespread use and applications The current existing Authenticated Routing for Ad Hoc Networks (ARAN) secure routing protocol is capable of defending itself against most malicious nodes and their different attacks. However, ARAN is not capable of defending itself against any authenticated selfish node participating in the network.

KEYWORDS: *Authenticated Routing for Ad Hoc Networks, essential security requirement, ARAN Default parameters, malicious and authenticated selfish nodes*

I. INTRODUCTION

A Mobile Ad Hoc Network (MANET) consists of a set of mobile hosts that carry out basic networking functions like packet forwarding, routing, and service discovery without the help of an established infrastructure. Nodes of an ad hoc network rely on one another in forwarding a packet to its destination, due to the limited range of each mobile host’s wireless transmissions. An ad hoc network uses no centralized administration. This ensures that the network will not cease functioning just because one of the mobile nodes moves out of the range of the others. Nodes should be able to enter and leave the network as they wish. Because of the limited transmitter range of the nodes, multiple hops are generally needed to reach other nodes. Every node in an ad hoc network must be willing to forward packets for other nodes. Thus, every node acts both as a host and as a router. The topology of ad hoc networks varies with time as nodes move, join or leave the network. This topological instability requires a routing protocol to run on each node to create and maintain routes among the nodes. Wireless ad-hoc networks can be deployed in areas where a wired network infrastructure may be undesirable due to reasons such as cost or convenience. It can be rapidly deployed to support emergency requirements, short-term needs, and coverage in undeveloped areas. So there is a plethora of applications for wireless ad-hoc networks. As a matter of fact, any day-to-day application such as electronic email and file transfer can be considered to be easily deployable within an ad hoc network environment. Also, we need not emphasize the wide range of military applications possible with ad hoc networks. Not to mention, the technology was initially developed keeping in mind the military applications, such as battlefield in an unknown territory where an infrastructure network is almost impossible to have or maintain. In such situations, the ad hoc networks having self-organizing capability can be effectively used where other technologies either fail or cannot be deployed effectively [21]. As a result, some well-known ad hoc network applications are:

- Collaborative Work: for some business environments, the need for collaborative computing might be more important outside office environments than inside. After all, it is often the case where people do need to have outside meetings to cooperate and exchange information on a given project.
- Crisis-management Applications: these arise, for example, as a result of natural disasters where the entire communications infrastructure is in disorder. Restoring communications quickly is essential. By using ad hoc networks, a communication channel could be set up in hours instead of days/weeks required for wire-line communications.
- Personal Area Networking and Bluetooth: a personal area network (PAN) is a short- range, localized network where nodes are usually associated with a given person. These nodes could be attached to someone's pulse watch, belt, and so on. In these scenarios, mobility is only a major consideration when interaction among several PANs is necessary.

MANETs have several significant characteristics and challenges. They are as follows:

- Dynamic topologies: Nodes are free to move arbitrarily. Thus, the network topology may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.
- Bandwidth-constrained, variable capacity links: Wireless links will continue to have significantly lower capacity than their hardwired counterparts. In addition, the realized throughput of wireless communications, after accounting for the effects of multiple access, fading, noise, and interference conditions, is often much less than a radio's maximum transmission rate.
- Energy-constrained operation: Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design optimization criteria may be energy conservation.

II. LITERATURE REVIEW

Security in MANET is an essential component for basic network functionalities like packet forwarding and routing. Network operation can be easily jeopardized if security countermeasures are not embedded into basic network functions at the early stages of their design. In mobile ad hoc networks, network basic functions like packet forwarding, routing and network management are performed by all nodes instead of dedicated ones. In fact, the security problems specific to a mobile ad hoc network can be traced back to this very difference. Instead of using dedicated nodes for the execution of critical network functions, one has to find other ways to solve this because the nodes of a mobile ad hoc network cannot be trusted in this way [2]. Fig. 3.1 illustrates the different attacks that can be made towards a network. [3,6].

2.1 Active and Passive Attacks

Security exposures of ad hoc routing protocols are due to two different types of attacks: active and passive attacks. In active attacks, the misbehaving node has to bear some energy costs in order to perform some harmful operation. In passive attacks, it is mainly about lack of cooperation with the purpose of energy saving. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered to be malicious while nodes that perform passive attacks with the aim of saving battery life for their own communications are considered to be selfish.

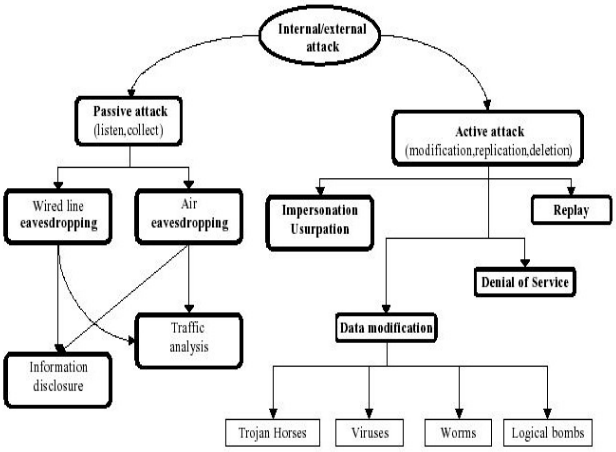

Fig.1: Different sorts of attacks

2.2 Malicious and Selfish Nodes in MANETs

Malicious nodes can disrupt the correct functioning of a routing protocol by modifying routing information, by fabricating false routing information and by impersonating other nodes. On the other side, selfish nodes can severely degrade network performances and eventually partition the network by simply not participating in the network operation.In existing ad hoc routing protocols, nodes are trusted in that they do not maliciously tamper with the content of protocol messages transferred among nodes. Malicious nodes can easily perpetrate integrity attacks by simply altering protocol fields in order to subvert traffic, deny communication to legitimate nodes (denial of service) and compromise the integrity of routing computations in general. As a result the attacker can cause network traffic to be dropped, redirected to a different destination or to take a longer route to the destination increasing communication delays. A special case of integrity attacks is spoofing whereby a malicious node impersonates a legitimate node due to the lack of authentication in the current ad hoc routing protocols. The main result of spoofing attacks is the misrepresentation of the network topology that possibly causes network loops or partitioning.

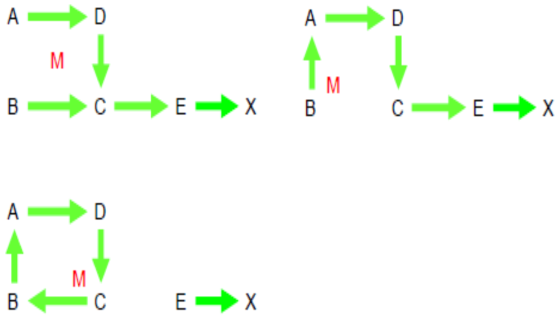

Fig. 2: Impersonation to create loops

In the above figure, a malicious attacker, M, can form a routing loop so that none of the four nodes can reach the destination. To start the attack, M changes its MAC address to match A's, moves closer to B and out of the range of A. It then sends an RREP to B that contains a hop count to X that is less than the one sent by C, for example zero. B therefore changes its route to the destination, X, to go through A. M then changes its MAC address to match B's, moves closer to C and out of range of B, and then sends to C an RREP with a hop count to X lower than what was advertised by E. C then routes to X through B. At this point a loop is formed and X is unreachable from the four nodes. Lack of integrity and authentication in routing protocols can further be exploited through "fabrication" referring to the generation of bogus routing messages. Fabrication attacks cannot be detected without strong authentication means and can cause severe problems ranging from denial of service to route subversion. A more subtle type of active attack is the creation of a tunnel (or wormhole) in the network between two colluding malicious nodes linked through a private connection bypassing the network. This exploit allows a node to short-circuit the normal flow of routing messages creating a virtual vertex cut in the network that is controlled by the two colluding attackers.

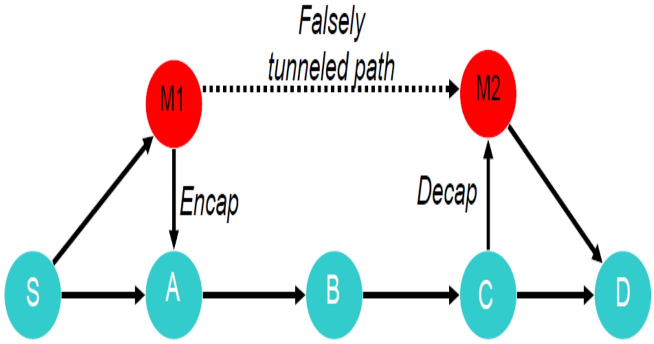

Fig. 3: Wormhole Attack

In the above figure, M1 and M2 are malicious nodes collaborating to misrepresent available path lengths by tunneling route request packets. Solid lines denote actual paths between nodes, the thin line denotes the tunnel, and the dotted line denotes the path that M1 and M2 falsely claim is between them. Let us say that node S wishes to form a route to D and initiates route discovery. When M1 receives a RDP from S, M1 encapsulates the RDP and tunnels it to M2 through an existing data route, in this case {M1->A->B->C->M2}. When M2 receives the encapsulated RDP, it forwards the RDP on to D as if it had only traveled {S->M1->M2->D}. Neither M1 nor M2 update the packet header to reflect that the RDP also traveled the path {A->B->C}. After route discovery, it appears to the destination that there are two routes from S of unequal length: {S->A->B->C->D} and {S- >M1->M2->D}. If M2 tunnels the RREP back to M1, S would falsely consider the path to D via M1 a better choice (in terms of path length) than the path to D via A.

Another exposure of current ad hoc routing protocols is due to node selfishness that results in lack of cooperation among ad hoc nodes. A selfish node that wants to save battery life, CPU cycles and bandwidth for its own communication can endanger the correct network operation by simply not participating in the routing protocol or by not forwarding packets and dropping them whether control or data packets. This type of attack is called the black-hole attack. Current Ad Hoc routing protocols do not address the selfishness problem and assumes that all nodes in the MANET will cooperate to provide the required network functionalities [2,4,5].

III. PROPOSED REPUTATION BASED AUTHENTICATION SCHEME

Performance of Mobile Ad Hoc Networks is well known to suffer from free-riding, selfish nodes, as there is a natural incentive for nodes to only consume, but not contribute to the services of the system. In the following, the definition of selfish behavior and the newly designed reputation-based scheme, to be integrated with normal ARAN routing protocol ending up having Reputed-ARAN, are presented.

3.1 Problem Definition

Whereas most of the attacks performed by malicious nodes can be detected and defended against by the use of the secure routing ARAN protocol, as was explained earlier, there remain the attacks that an authenticated selfish node can perform.

There are two attacks that an authenticated selfish node can perform that the current ARAN protocol cannot defend against. To illustrate these two possible attacks that a selfish node can use to save its resources in a MANET communication that allows the categorization of attacks that lead an attacker to reach a specific goal is used. In the below table, the attack tree that cannot be detected by current ARAN protocol is shown:

Table 1: Attack Tree: Save own resources

Attack tree: Save own resources
OR 1. Do not participate in routing
1. Do not relay routing data

OR 1. Do not relay route requests
2. Do not relay route replies
2. Do not relay data packets
1. Drop data packets

All the security features of ARAN fail to detect or defend against these attacks, as they focus only on the detection of malicious nodes' attacks and not the authenticated selfish nodes' attacks. ARAN protocol assumes that authenticated nodes are to cooperate and work together to provide the routing functionalities.

3.2 Proposed Reputation-based Scheme

3.2.1 Introduction

As nodes in mobile ad hoc networks have a limited transmission range, they expect their neighbors to relay packets meant for far off destinations. These networks are based on the fundamental assumption that if a node promises to relay a packet, it will relay it and will not cheat. This assumption becomes invalid when the nodes in the network have tangential or contradictory goals. The reputations of the nodes, based on their past history of relaying packets, can be used by their neighbors to ensure that the packet will be relayed by the node. In the upcoming subsections, a discussion of a simple reputation-based scheme to detect and defend against authenticated selfish nodes' attacks in MANETs built upon the ARAN protocol is presented. Sometimes authenticated nodes are congested and they cannot fulfill all control packets broadcasted in the MANET so they choose not to reply to other requests in order to do their own assigned load according to their battery, performance and congestion status. My scheme do not forward control packets, by considering the reputation value of the node asking others to forward its packets. If the packet has originated from a low-reputed node, the packet is put back at the end of the queue of the current node and if the packet has originated from a high-reputed node, the current node sends the data packet to the next hop in the route as soon as possible. This scheme helps in encouraging the nodes to participate and cooperate in the ad hoc network effectively. Moreover attacks in which authenticated nodes promise to route data packets by replying to control packets showing their interest in cooperation in forwarding these data packets but then they become selfish and start dropping the data packets. This is done by giving incentives to the participating nodes for their cooperation. The proposed scheme is called Reputed-ARAN. Different from global indirect reputation-based schemes like Confidant and Core, the proposed solution uses local direct reputations only like in Ocean reputation-based scheme. Each node keeps only the reputation values of all direct nodes it dealt with. These reputation values are based on the node's firsthand experience with other nodes. My work is partially following the same methodology about reputation systems for AODV.

3.2.2 Design Requirements

The following requirements are set while designing the reputation-based scheme to be integrated with the ARAN protocol:

- The reputation information should be easy to use and the nodes should be able to ascertain the best available nodes for routing without requiring human intervention.
- The system should not have a low performance cost because low routing efficiency can drastically affect the efficiency of the applications running on the ad hoc network.
- Nodes should be able to punish other selfish nodes in the MANET by providing them with a bad reputation.
- The system should be built so that there is an injection of motivation to encourage cooperation among nodes.
- The collection and storage of nodes' reputation values are done in a decentralized way.
- The system must succeed in increasing the average throughput of the mobile ad hoc network or at least maintain it.

3.2.3 Main Idea of the Reputation System

In the proposed reputation scheme, all the nodes in the mobile ad hoc network will be assigned an initial value of null (0) as in the Ocean reputation-based scheme. Also, the functionality of the normal

ARAN routing protocol in the authenticated route setup phase will be modified so that instead of the destination unicasts a RREP to the first received RDP packet of a specific sender only, the destination will uncast a RREP for each RDP packet it receives and forward this RREP on the reverse-path. The next-hop node will relay this RREP. This process continues until the RREP reaches the sender. After that, the source node sends the data packet to the node with the highest reputation. Then the intermediate node forwards the data packet to the next hop with the highest reputation and the process is repeated till the packet reaches its destination. The destination acknowledges the data packet (DACK) to the source that updates its reputation table by giving a recommendation of (+1) to the first hop of the reverse path. All the intermediate nodes in the route give a recommendation of (+1) to their respective next hop in the route and update their local reputation tables. If there is a selfish node in the route, the data packet does not reach its destination. As a result, the source does not receive any DACK for the data packet in appropriate time. So, the source gives a recommendation of (-2) to the first hop on the route. The intermediate nodes also give a recommendation (-2) to their next hop in the route up to the node that dropped the packet. As a consequence, all the nodes between the selfish node and the sender, including the selfish node, get a recommendation of (-2). The idea of giving (-2) to selfish nodes per each data packet dropping is due to the fact that negative behavior should be given greater weight than positive behavior. In addition, this way prevents a selfish node from dropping alternate packets in order to keep its reputation constant. This makes it more difficult for a selfish node to build up a good reputation to attack for a sustained period of time [23]. Moreover, the selfish node will be isolated if its reputation reached a threshold of (-40) as in the Ocean reputation-based scheme. In the following table, the default Reputed-ARAN parameters are listed:

Table 2: Reputed-ARAN Default parameters

Initial Reputation	0
Positive Recommendation	+1
Negative Recommendation	-2
Self fish Drop Threshold	-40
Re-induction Time out	5 Minutes

The proposed protocol will be structured into the following four main phases, which will be explained in the subsequent subsections:

- Route Lookup Phase
- Data Transfer Phase
- Reputation Phase
- Timeout Phase

3.2.3.1 *Route Lookup Phase*

This phase mainly incorporates the authenticated route discovery and route setup phases of the normal ARAN secure routing protocol. In this phase, if a source node S has packets for the destination node D, the source node broadcasts a route discovery packet (RDP) for a route from node S to node D. Each intermediate node interested in cooperating to route this control packet broadcasts it throughout the mobile ad hoc network; in addition, each intermediate node inserts a record of the source, nonce, destination and previous-hop of this packet in its routing records. This process continues until this RDP packet reaches the destination. Then the destination unicasts a route reply packet (RREP) for each RDP packet it receives back using the reverse-path. Each intermediate node receiving this RREP updates its routing table for the next-hop of the route reply packet and then unicasts this RREP in the reverse-path using the earlier-stored previous-hop node information. This process repeats until the RREP packet reaches the source node S. Finally, the source node S inserts a record for the destination node D in its routing table for each received RREP.

In the below fig., the route lookup phase is presented in details, illustrating the two phases of it, the authenticated route discovery phase and the authenticated route setup phase.

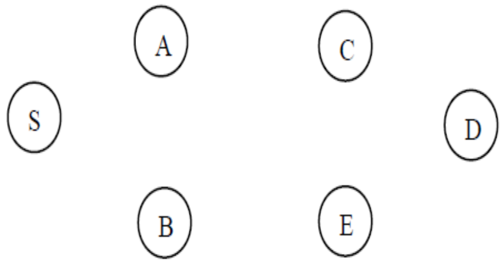

Fig. 4: A MANET Environment

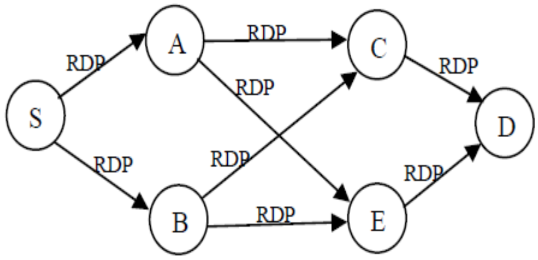

Fig. 5: Broadcasting RDP

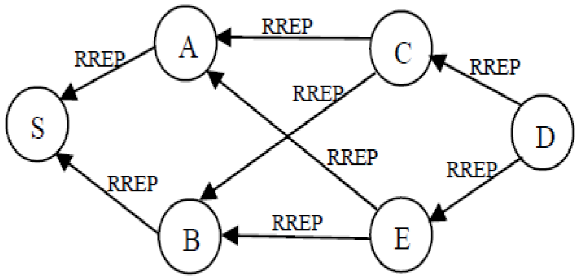

Fig. 6: Replying to each RDP

3.2.3.2 ***Data Transfer Phase***

At this time, the source node S and the other intermediate nodes have many RREPs for the same RDP packet sent earlier. So, the source node S chooses the highly-reputed next-hop node for its data transfer. If two next-hop nodes have the same reputation, S will choose one of them randomly, stores its information in the sent-table as the path for its data transfer. Also, the source node will start a timer before it should receive a data acknowledgement (DACK) from the destination for this data packet. Afterwards, the chosen next-hop node will again choose the highly-reputed next-hop node from its routing table and will store its information in its sent-table as the path of this data transfer. Also, this chosen node will start a timer, before which it should receive the DACK from the destination for this data packet. This process continues till the data packet reaches the destination node D. And of course in this phase, if the data packet has originated from a low-reputed node, the packet is put back at the end of the queue of the current node. If the packet has originated from a high-reputed node, the current node sends the data packet to the next highly-reputed hop in the route discovered in the previous phase as soon as possible. Once the packet reaches its destination, the destination node D sends a signed data acknowledgement packet to the source S. The DACK traverses the same route as the data packet, but in the reverse direction.

In the following fig., the data transfer phase is illustrated:

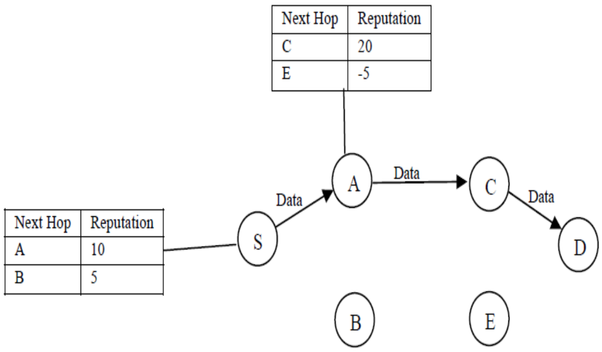

Fig. 7: Choosing the highly-reputed next-hop node

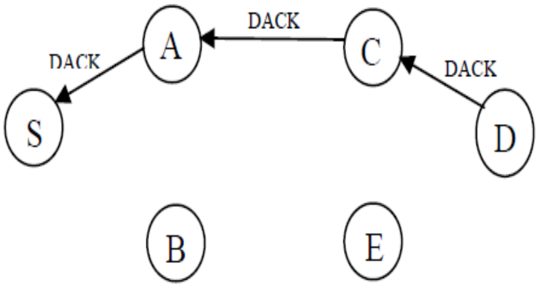

Fig.8: Sending Data Acknowledgement for each received data packet

3.2.3.3 *Reputation Phase*

In this phase, when an Intermediate node receives a data acknowledgement packet (DACK), it retrieves the record, inserted in the data transfer phase, corresponding to this data packet then it increments the reputation of the next hop node. In addition, it deletes this data packet entry from its sent-table. Once the DACK packet reaches node S, it deletes this entry from its sent-table and gives a recommendation of (+1) to the node that delivered the acknowledgement.

3.2.3.4 Timeout Phase

In this phase, once the timer for a given data packet expires at a node; the node retrieves the entry corresponding to this data transfer operation returned by the timer from its sent-table. Then, the node gives a negative recommendation (-2) to the next-hop node and deletes the entry from the sent-table. Later on, when the intermediate nodes' timers up to the node that dropped the packet expire, they give a negative recommendation to their next hop node and delete the entry from their sent-table. As a consequence, all the nodes between the selfish node and the sender, including the selfish node, get a recommendation of (-2). Now, if the reputation of the next-hop node goes below the threshold (-40), the current node deactivates this node in its routing table and sends an error message RERR to the upstream nodes in the route. Then the original ARAN protocol handles it. Now, it is the responsibility of the sender to reinitiate the route discovery again. In addition, the node whose reputation value reached (-40) is now temporally weeded out of the MANET for five minutes and it later joins the network with a value of (0) so that to treat it as a newly joined node in the network.

IV. CONCLUSION

A comparison between some the existing secure mobile ad hoc routing protocols was presented. Then, an in-depth talk about the Authenticated Routing for Ad Hoc Networks protocol (ARAN) as one of the secure routing protocols built following the fundamental secure routing protocols design methodology was given. Afterwards, a discussion of how ARAN defends against most of the attacks that are conducted by malicious nodes such as spoofing, fabrication, modification and disclosure ones was presented. That resulted in proving that the currently existing specification of the ARAN secure routing MANET protocol does not defend against attacks performed by authenticated selfish nodes. Thus, I moved on discussing the different existing MANET cooperation enforcement schemes by stating their types: the virtual currency-based and the reputation-based schemes. In this proposal, the different phases of the proposed reputation-based scheme were explained. Then, an analysis of the various forms of selfish attacks that the proposed reputation-based scheme defends against was presented. Also, some time was invested in surveying the different simulation packages that are used in mobile ad hoc networks. The solution presented in this thesis only cover a subset of all threats and is far from providing a comprehensive answer to the many security problems in the MANETs field. Last but not least, according to the many simulations that were performed, the newly proposed reputation-based scheme, built on top of normal ARAN secure routing protocol, achieves a higher throughput than the normal ARAN in the presence of selfish nodes. Thus, the proposed design, Reputed-ARAN, proves to be more efficient and more secure than normal ARAN secure routing protocol in defending against both malicious and authenticated selfish nodes.

REFERENCES

[1] R.PushpaLakshmi and Dr.A.Vincent Antony Kumar, "Security aware Minimized Dominating Set based Routing in MANET", IEEE 2010 Second International conference on Computing, Communication and Networking Technologies. Dept. of Inf. Technol.,PSNA Coll. of Eng. & Technol., India,pp. 1 – 5, July 2010.
[2] G. Lavanya, C.Kumar And A. Rex Macedo Arokiaraj, "Secured Backup Routing Protocol For Ad Hoc Networks', IEEE International Conference on Signal Acquisition and Processing. Bangalore, India , pp.45-50, 2010.
[3] YongQing Ni, DaeHun Nyang and Xu Wang, "A-Kad: an anonymous P2P protocol based on Kad network", IEEE 2009. Inf. Security Res. Lab., Inha Univ., Incheon, South Korea , pp. 747 – 752, 2009.
[4]N.Bhalaji,Dr.A.Shanmugam,"Association Betwwen Nodes To Combat Blackhole Attack In Dsr Based Manet", Wireless and Optical Communications Networks,WOCN., IEEE 2009 IFIP International Conference on Cairo ,pp.1-5 ,2009 .
[5] Sohail Jabbar, Abid Ali Minhas, Raja Adeel Akhtar, Muhammad Zubair Aziz, "REAR: Real-Time Energy Aware Routing for Wireless Adhoc Micro Sensors Network", Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing pp. 825-830, 2009.
[6] D.Suganya Devi and Dr.G.Padmavathi, "Performance Efficient EOMCT Algorithm for Secure Multicast Key Distribution for Mobile Adhoc Networks", IEEE International Conference on Advances in Recent Technologies in Communication and Computing. pp 1-25, 2009.
[7] Jian Ren and Yun Li and Tongtong Li, "Providing Source Privacy in Mobile Ad Hoc Networks" , IEEE, Macau SAR, P.R.China,PP. 12-15 ,2009.
[8] Matthew Tan Creti, Matthew Beaman, Saurabh Bagchi, Zhiyuan Li, and Yung-Hsiang Lu, Multigrade Security Monitoring for Ad-Hoc Wireless Networks", IEEE 6th International Conference on Mobile Adhoc and Sensor Systems , Pages: 342-352,2009.
[9] S. Zhong, J. Chen, and Y. Yang. Sprite: A simple, Cheat-proof, Credit-based System for Mobile Ad hoc Networks. Proceedings of IEEE Infocom, , pages 1987-1997, April 2003.
[10] L. Zhou and Z. Haas. Securing Ad Hoc Networks. IEEE Networks Special Issue on Network Security. Vol. 13, no. 6, pages 24-30 ,December 1999.
[11] Wenchao Huang, Yan Xiong, Depin Chen, "DAAODV: A Secure Ad-hoc Routing Protocol based on Direct Anonymous Attestation", IEEE 2009 International Conference on Computational Science and Engineering, pp 809-816,2009.
[12] A.H Azni, Azreen Azman, Madihah Mohd Saudi, AH Fauzi, DNF Awang Iskandar, "Analysis of Packets Abnormalities in Wireless Sensor Network" , IEEE 2009 Fifth International Conference on MEMS NANO, and Smart Systems, pp 259-264,2009.
[13] Cuirong Wang, Shuxin Cai, "AODVsec: A Multipath Routing Protocol in Ad-Hoc Networks for Improving Security", IEEE 2009 International Conference on Multimedia Information Networking and Security, pp 401-404,2009.
[14] A Nagaraju and B.Eswar, "Performance of Dominating Sets in AODV Routing protocol for MANETs", IEEE 2009 First International Conference on Networks & Communications, pp 166-170,2009.
[15] Sheng Cao and Yong Chen, "AN Intelligent MANet Routing Method MEC", 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, pp 831-834.
[16] WANG Xiao-bo ,YANG Yu-liang, AN Jian-wei, "Multi-Metric Routing Decisions in VANET", 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, PP 551-556,2009.
[17] Zeyad M. Alfawaer and Saleem Al_zoubi, "A proposed Security subsystem for Ad Hoc Wireless Networks", IEEE 2009 International Forum on Computer Science-Technology and Applications, Volume 02, pp 253-256, 2009.
[18] Shayesteh Tabatabaei, "Multiple Criteria Routing Algorithms to Increase Durability Path in Mobile Ad hoc Networks", IEEE 2009 by the Institute of Electrical and Electronics Engineers. PP. 1 – 5, Nov.2009.

[19] Cuirong Wang, Shuxin Cai, and Rui Li, "AODVsec: A Multipath Routing Protocol in Ad-Hoc Networks for Improving Security", IEEE 2009 International Conference on Multimedia Information Networking and Security, Northeastern Univ. at Qinhuangdao China ,Volume: 2, pp 401-404,2009.
[20] A Nagaraju and B.Eswar, "Performance of Dominating Sets in AODV Routing protocol for MANETs", IEEE 2009 First International Conference on Networks & Communications, pp 166-170,2009.
[21] Tirthankar Ghosh, Niki Pissinou, Kia Makki, "Collaborative Trust-based Secure Routing Against Colluding Malicious Nodes in Multi-hop Ad Hoc Networks", 29th Annual IEEE International Conference on Local Computer Networks (LCN'04). pp.224-231,USA,2009.
[22] M. F. Juwad, and H. S. Al-Raweshidy, "Experimental Performance Comparisons between SAODV & AODV", IEEE 2008 Second Asia International Conference on Modelling & Simulation, pp 247-252,2008.
[23] Wei Ren, Yoohwan Kim, Ju-Yeon Jo, Mei Yang3 and Yingtao Jiang, "IdSRF: ID-based Secure Routing Framework for Wireless Ad-Hoc Networks", IEEE 2007 International Conference on Information Technology (ITNG'07) , pp.102-110,2007.
[24] Anand Patwardhan and Michaela Iorga, "Secure Routing and Intrusion Detection in Ad Hoc Networks", 3rd IEEE Int'l Conf. on Pervasive Computing and Communications
(PerCom 2005). University of Maryland - Baltimore County, pp.191-199,2005.

Authors

Abdalrazak T. Rahem pursuing Mtech from Information Technology Department at Bharati Vidyapeeth Deemed University College of Engineering, Dhankawadi, Pune India. His areas of interest are Software Engineering and networks .

H K Sawant is working as an Professor in Information Technology Department at Bharati Vidyapeeth Deemed University College of Engineering, Dhankawadi, Pune India. He was awarded his Master of Technology Degree from IIT Mumbai. He is pursuing his PhD from JJTU. His areas of interest are Computer Network, Software Engineering and Multimedia System. He has nineteen years experience in teaching and research. He has published more than twenty research papers in journals and conferences. He has also guided ten postgraduate students.