GRILLING GRATUITOUS DETOUR IN ADHOC NETWORK

S. Vijayalakshmi[1], S.Albert Rabara[2]

[1] Senior Lecturer, Department of Computer Applications, IFET College of Engineering,Villupuram, anviji_lakshmi@yahoo.co.in

[2] Professor, Department of Computer Science, St. Josephs College, Bharathidasan University, Trichy, a_rabara@yahoo.com

ABSTRACT

Routing is a critical function in adhoc network which claim special attention and support extended by the trustable neighbor nodes. The peril of Gratuitous detour on routing process in ad hoc network is manifold which culminates in the deterioration of network performance amounting to deplorable network behavior. Routing in ad hoc network is a cooperative process as it requires periodic assistance from the intermediate nodes to route the packets to the far off nodes that are beyond the direct wireless transmission range. The role of intermediate nodes in routing is crucial and it mandates special attention and support from the sender node and as well the good Samaritan neighboring nodes. This paper advocates the creation of two lists namely PFL and SFL backed by Dominant Pruning Method. The misbehaving middle node exhibiting Gratuitous Detour (GD) has to be curtailed by performing a cardinality operation on the route cache (storing the intermediate nodes enroute to the destination) of the nodes in PFL and SFL. The sender node stringent process of recruiting the genuine intermediate nodes in both the list is echoed periodically by performing a cardinal operation to restrain the occurrence of GD which manifest by projecting a non existent node or concealing an existent node. The result of the cardinal operation approves the truth that the nodes in Route cache (Buffered Route Path) are genuine or not. The proposed solution demands a heavy pay from the M^3N whose intention is either to disrupt the optimal routing process by hiding a potential peer after launching a blackmail or DoS attack on it. The ulterior motive of the Malicious Misbehaving Middle (M^3N) in projecting the non existent nodes (Longer Virtual Route) to evade the role of routing intermediary is also effectively thwarted. Suitable graph have been simulated to study the effect of mobility and no. of misbehaving nodes on the Sender Node Probing Latency Index (SNPLI).

KEYWORDS

MANET, Gratuitous Detour, Primary Forwarding List, Secondary Forwarding List

1. INTRODUCTION

A mobile ad-hoc network (MANET) may be defined as a collection of mobile hosts, which maintain interconnection without the intervention of a centralized access point. To facilitate multi-hop communication between non- neighbor nodes, other nodes must act as routers. Network nodes in MANETs are free to move randomly. Therefore, the network topology of a MANET may change rapidly and unpredictably. All network activities such as discovering the topology and delivering data packets have to be executed by the nodes themselves, either individually or collectively. Since MANETs can be set up easily and inexpensively, they have a wide range of applications especially in military operation and emergency and disaster relief effort. MANETs are more vulnerable to security attacks than conventional wired and wireless

DOI : 10.5121/ijdps.2011.2204

networks due to the open wireless medium used, dynamic topology, distributed and cooperative sharing of channels and other resources, power and computation constraints [1].

Routing has always been one of the key challenges in MANETs and the challenge becomes more difficult when the network size increases. In MANETs an individual node may attempt to benefit from other nodes, but refuse to share its own resource. Such nodes are known as selfish nodes and their behavior is termed as selfish or misbehavior. One of the major sources of the energy consumption in mobile nodes of MANETs is wireless transmission. A selfish node may refuse to forward data packets for other nodes in order to conserve its energy. A malicious node introduces a denial of service attack by dropping packets [2]. A broken node prevents it from forwarding packets by having a software fault. Several security techniques have been proposed, but the system may misbehave when an attacker enters into the network and reduces the network performance. These nodes do not forward packets properly. They may drop the packets that forward across them or declare a faulty routing updates. Other attacks such as the information can be read by the unauthorized persons in the network or modified by the attacker nodes [3][4].

The objective of this paper is to highlight the plight of the ad hoc network routing inflicted by the Gratuitous Detour (GD) a serious route malfunction looming the network performance and throughput. This paper advocates the means to safeguard the sender nodes from falling prey to this misbehaving intermediate node by insisting on the creation of Primary Forwarding List (PFL) and Secondary Forwarding List (SFL) backed by Dominant Pruning Method. The nodes in both lists periodically handshake with each other to prune the non existent nodes and uncover the hidden nodes in the route cache of the intermediate nodes. This paper also insists on performing a cardinal operation on the buffered Route Cache of intermediate nodes enroute to destination. The value returned for the cardinal operation illustrates the factual network position.

1.1. Reading Roadmap

The rest of the paper is organized as follows. **Section 2** presents a survey of security issues of routing in MANET. In **Section 3**, we provide discussion on the resilient counter strategy to grill gratuitous detour in ad hoc network. **Section 4** expounds the simulation study using Network Simulator. Finally, we make some conclusions and future direction in **Section 5**.

2. RELATED WORK

Pathan, K.S.A. et al [3] proposed an efficient routing protocol for ad hoc networks which we named NAMP (Neighbor Aware Multicast Routing Protocol). NAMP aims at achieving higher performance by reducing control overhead and improvement of the end-to-end delivery of data packets. It is a tree based, hybrid multicast routing protocol. For route creation, NAMP uses the neighboring information and dominant pruning approach. It uses secondary forwarder method for route maintenance.

Hu, C.Y. et al [4] highlights that ad hoc networks use mobile nodes to enable communication outside wireless transmission range. Attacks on ad hoc network routing protocols disrupt network performance and reliability. The authors survey the state of research and its challenges in this field.

Hu, C.Y. et al [5] present attacks against routing in ad hoc networks, and we present the design and performance evaluation of a new secure on-demand ad hoc network routing protocol, called Ariadne. Ariadne prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents a large number of types of Denial-of-Service attacks. In addition, Ariadne is efficient, using only highly efficient symmetric cryptographic primitives.

Marti, S. et al [11] describe two techniques that improve throughput in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so. To mitigate this problem, we propose categorizing nodes based upon their dynamically measured behavior. We use a watchdog that identifies misbehaving nodes and a path rater that helps routing protocols avoid these nodes. Through simulation we evaluate watchdog and path rater using packet throughput, percentage of overhead (routing) transmissions, and the accuracy of misbehaving node detection.

Vijayalakshmi, S. et al [13] discusses the implications of the Byzantine attack in the online auction Network have been studied. Besides the existing network performance parameters like delay, jitter, throughput, Packet Delivery Ratio (PDR) another parameter by name Immediate Neighbor Aware Vouch Count (INAVC) is included to proactively select a fault free multicast route. This proactive parameter is dynamic and reflects the true multicast architecture in adhoc network thereby enabling to instantly prune the Byzantine adversary. Providing robust and resilient defense solutions to subvert this attack in auction Network becomes the focus of this paper.

Iyengar, N.C.S.N. et al [14] introduces the concept of random routing algorithm that neither maintains a routing table nor floods the entire network as done by various known protocols thereby reducing the load on network in terms of number of control packets in a highly dynamic scenario. This paper calculates the expected run time of the designed random algorithm.

Imran, N. et al [15] propose a gossip based protocol that consumes little resources. Our proposed scheme aims to keep the routing table size R as low as possible yet it ensures that the diameter is small too. We learned the performance of our proposed protocol through simulations. Results show that our proposed protocol attains major improvement in network reachability and connectivity.

3. SURVEY OF SECURITY ISSUES OF ROUTING IN MANET

Attacks on an ad hoc network routing protocols generally fall into one of two categories: *routing disruption* attacks and *resource consumption* attacks. In a routing disruption attack, the attacker attempts to cause legitimate data packets to be routed in dysfunctional ways. In a resource consumption attack, the attacker injects packets into the network in an attempt to consume valuable network resources such as bandwidth, or to consume node resources such as memory (storage) or computation power [5]. From an application layer perspective, both attacks are instances of a Denial-of-Service (DoS) attack. An example of a routing disruption attack is for an attacker to send forged routing packets to create a *routing loop*, causing packets to traverse nodes in a cycle without reaching their destinations, consuming energy and available bandwidth. An attacker may similarly create a routing black hole, in which all packets are dropped: by sending forged routing packets, the attacker could route all packets for some destination to itself and then discard them, or the attacker could cause the route at all nodes in an area of the network to point “into” that area when in fact the destination is outside the area. As a special case of a black hole, an attacker could create a gray hole, in which it selectively drops some packets but not others, for example, forwarding routing packets but not data packets. An attacker may also attempt to cause a node to use detours (suboptimal routes) or may attempt to partition the network by injecting forged routing packets to prevent one set of nodes from reaching another [6][7]. An attacker may attempt to make a route through itself appear longer by adding virtual nodes to the route; we call this attack gratuitous detour, as a shorter route exists and would otherwise have been used. In ad hoc network routing protocols that attempt to keep track of perceived malicious nodes in a “blacklist” at each node, such as is done in watchdog and path rater, an attacker may blackmail a good node, causing other good nodes to add that node to their blacklists, thus avoiding that node in routes.

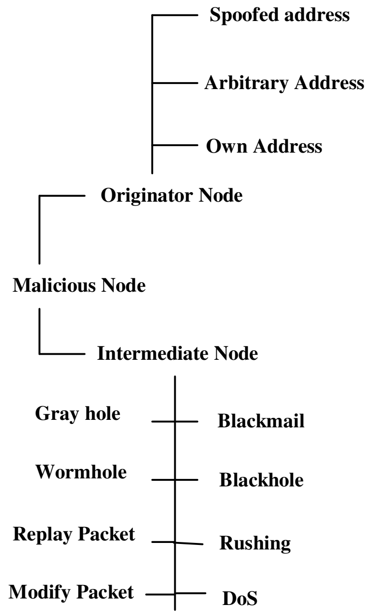


Figure 1: Classification of Attack in MANET

A more subtle type of routing disruption attack is the creation of a wormhole in the network. A wormhole attack typically requires the presence of at least two colluding nodes in an ad hoc network. The malicious nodes need to be geographically separated in order for the attack to be effective. In this attack, a malicious node captures packets from one location and “tunnels” these packets to the other malicious node, which is assumed to be located at some distance [8] [15]. The second malicious node is then expected to replay the “tunneled” packets locally. The rushing attack is a malicious attack that is targeted against on-demand routing protocols that use duplicate suppression at each node. An attacker disseminates ROUTE REQUESTs quickly throughout the network, suppressing any later legitimate ROUTE REQUESTs when nodes drop them due to the duplicate suppression [9]. An example of a resource consumption attack is for an attacker to inject extra data packets into the network, which will consume bandwidth resources when forwarded, especially over detours or routing loops. Similarly, an attacker can inject extra control packets into the network, which may consume even more bandwidth or computational resources as other nodes process and forward such packets [10][16]. DoS attack is one where the attacker sends a single packet that results in a packet flood throughout the network.

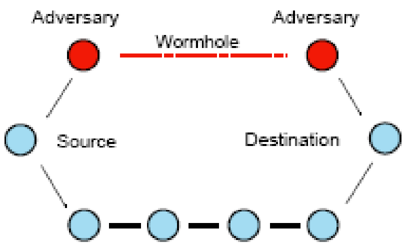


Figure 2: Simple Wormhole Configuration

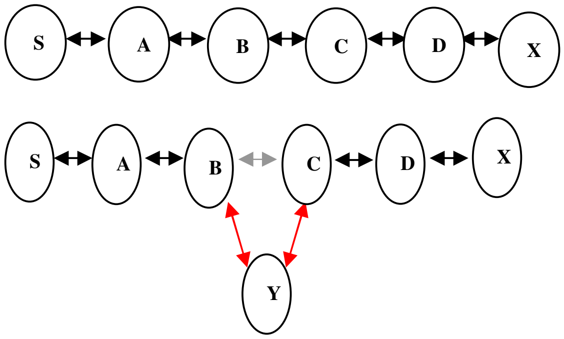


Figure 3: Conceptual View of Gratuitous Detour

3. RESILIENT COUNTER STRATEGY TO GRILL GRATUITOUS DETOUR

Deployment of Ad hoc networks is inevitable in this resource constrained computing environment. This necessitates an optimal utilization/implementation of this network. The networks with its unique features augment the high end technological advancements and the proliferation of hand held devices to realize high performance computing. The peer-to-peer architecture of this network mandates each node to win the confidence of its neighbor and build trust relationship with it. This helps the nodes to reach the other indirect nodes through the genuine intermediate node. So routing in ad hoc network is obviously a cooperative process which needs holistic support from immediate neighbors. This interesting requirement throws open a host of security challenges unfolded by the malicious intermediate nodes transcending the network boundaries to sustain reachability and accessibility. The susceptible nature of this network solicit an opportunity to usurp the resources associated with this network by launching an sting of attacks like Black hole, Gray hole, Rushing attack, Wormhole attack, Detour, GD etc. This paper aims at proposing a robust solution to counter the threats posed on this network by the GD technique and analyze the impact [11].

GD is a technique in which the trusted intermediate node misbehaves by projecting a virtual suboptimal/super optimal route through it [17]. This is manifested by virtually adding a node that is either non existent or conceals an existing node from the RREQ and RREP packet from the genuine neighbors. The main intention of this technique is not to jeopardize the ongoing routing process but to remain selfish to evade the role of routing intermediary and to get an undue share of data. The general tendency of any sender node is to select only routes with minimal route metrics which obviate the inclusion of this node as an intermediary had it resorted to project a fairly longer route than the original route. There is possibility for sender to notice the service of intermediate nodes if the advertised RREQ and RREP packets contain lesser metric by covering/hiding certain nodes by launching a blackmail/DoS attack on it.

Any node wishing to invoke a route to any destination requires the creation of two lists (PFL and SFL) using Dominant Pruning Method (DPM) [12]. The resulting routing mesh structure helps in the prompt delivery of packets to the intended destination despite the presence of substantial adversaries. This compels the sender to seek the service of GNS (Genuine Neighbor Set) to validate the selection/participation of intermediate nodes in either the PFL/SFL. The various parameters deployed for this purpose include Further Route Request (FRREQ), Further Route Response (FRREP), Route Confirmation Request (CRREQ) and Route Confirmation Reply (CRREP) etc.

DPM discusses an efficient routing protocol for ad hoc network named as NAMP (Neighbor Aware Multicast Routing Protocol) [13] [14]. NAMP aims at achieving higher performance by reducing control overhead and improvement of the end-to- end delivery of data packets. It is a tree based, hybrid multicast routing protocol. NAMP uses the neighboring information and dominant pruning approach for route creation. The inclusion of intermediate nodes in PFL ascertains the fact that the node is free from all routing influences mainly GD. This may not hold good always as the selected PFL node may misbehave at any point of time. This intermittent misbehavior is spotted by the (always alert active) A^3 nodes present in SFL and GNS nodes. The very mere presence of nodes in PFL and SFL compounds the fact that it have not so far yielded to the adversary pressure amounting to a compromised status.

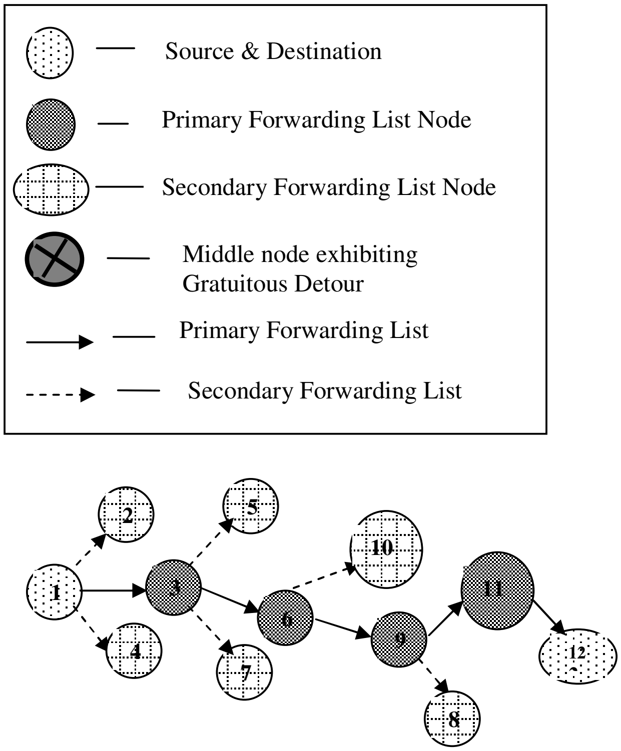
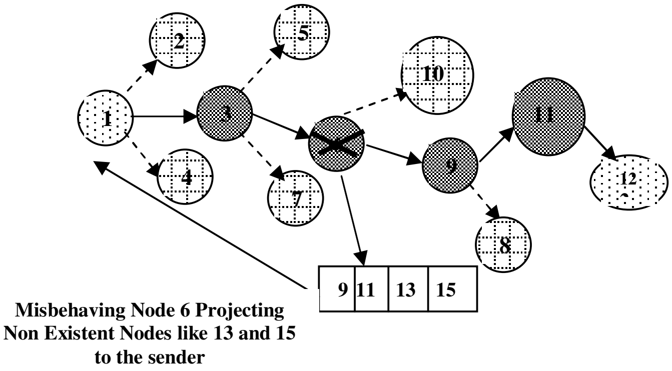

Source & Destination
Primary Forwarding List Node
Secondary Forwarding List Node
Middle node exhibiting Gratuitous Detour
Primary Forwarding List
Secondary Forwarding List
2
5
10
1
3
11
6
9
12
4
7
8

Figure 4: Formation of SFL



Misbehaving Node 6 Projecting Non Existent Nodes like 13 and 15 to the sender

Figure 5: PFL Node 6 exhibiting Gratuitous Detour

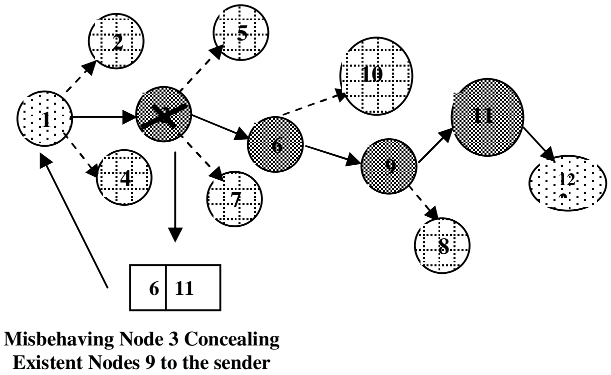

1
2
3
4
5
6
7
8
9
10
11
12
6 11
Misbehaving Node 3 Concealing Existent Nodes 9 to the sender

Figure 6: PFL Node 3 exhibiting Gratuitous Detour

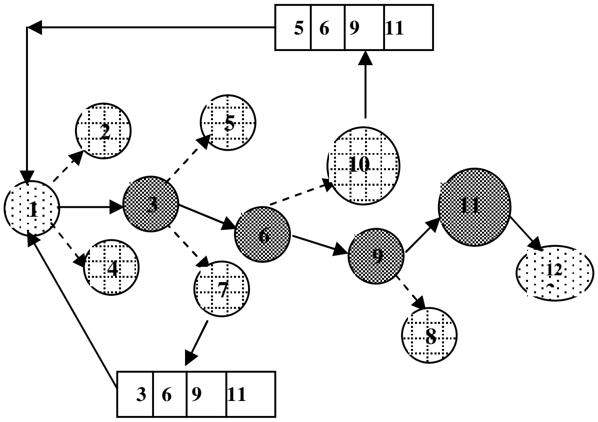


Figure 7: SFL Nodes periodically forwarding Buffered Route Cache to check Gratuitous Detour

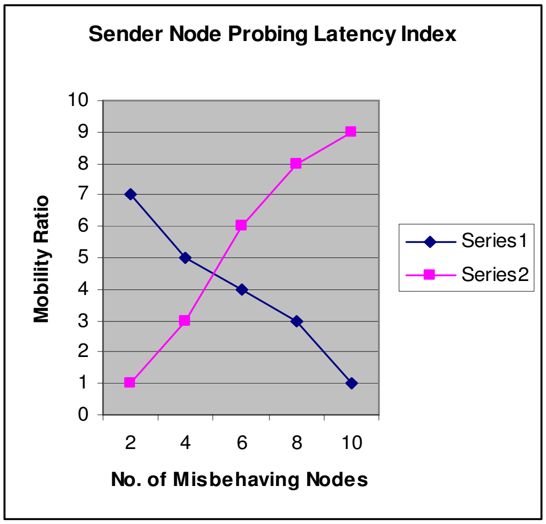
As routing is a cooperative and coordinated process, both PFL and SFL nodes complement each other in its operation of targeting the Malicious Misbehaving Middle (M^3N) node which is exhibiting GD. The sender on receipt of RREP packets which contain route metric details like hop count, transmission delay etc. from the PFL does not immediately accept it. Instead it checks for the cardinality of the node presence in SFL nodes and the GNS nodes to validate the possibility of inclusion of the middle node’s RREP as genuine or forged. The null value in cardinal operation signifies the fact that the intermediate node is trying to play spoil sport by projecting a non existent node’s identity. This can also be construed as obscuring the existence of node which is very much present either in PFL or SFL by mounting a DoS attack or blackmail attack on it. Figures 4 to 7 highlight the malicious behaviour exhibited by middle node in concealing the existent nodes and projecting non existent nodes in ad hoc routing.

The high value returned for the cardinal operation attest to the fact that the intermediate node in PFL is not really interested in forwarding the transient packets to other nodes. Hence it forges the identities of the existing node or orchestrate arbitrary node with virtual identities and deploy it to participate in the routing process. The resulting route engaging the duplicated nodes projects itself as a costly node thereby remaining elusive and detrimental to the conduct of the normal routing process. The respective node cardinality checking is achievable using the NEIGHBOR NODE ROUTE CACHE WATCH SYSTEM (N^2RCWS) as the nodes in PFL and

SFL maintains the discovered route in its cache for future use and deployment. This system is also backed by N^3 (Neighbor to Neighbor Nexus) which collaboratively work together to achieve the expected network performance. The route caching becomes handy to detect the breach able node that is violating the well laid prior security policies and rules during the negotiation of security association.

4. SIMULATION STUDY

The GD routing malpractice in ad hoc network can be initially prohibited by making the participating nodes to pass through various criteria like CRREQ, FRREQ, FRREP etc. Only the nodes which have a clearance affidavit from the other nodes can be positioned in either PFL or SFL. The mid misbehaviour of the nodes due to GD can be captured by the high or low value returned by the cardinality operation performed on the Neighbor Node Route Cache. The sender can grew suspicious if the value returned is not truly reflecting the present network condition and state. This security problem is compounded by the mobility of wireless nodes which weakens the probing/grilling power of the sender or GNS nodes. The nodes exhibiting high mobility ratio has higher chance of getting trapped by the probing node due to the closed network nexus. Therefore higher mobility quotient of the nodes in PFL encourages the node probing latency time. The nodes with lower mobility quotient have lean possibility of being viewed by other neighboring probing nodes which fail to produce a conviction report of the misbehaving nodes exhibiting GD. Thus the mobility of the node catalyzes the mitigation of routing misbehavior in ad hoc network. A graph is drawn with no. of misbehaving nodes on X axis and the mobility quotient on Y axis. It is clearly evident from the graph that mobility quotient increases the possibility of detection quotient of the misbehaving node. This graph containing the two disjoint lines interprets the network position in the presence of Gratuitous Detour routing anomaly. Series 2 expounds the fact that the increase in mobility ratio of nodes triggers the sender node in captivating the spurious node exhibiting Gratuitous Detour. Similarly Series 1 displays the plummeting nature of mobility ratio which has serious implications on the sender node in zeroing in on the node causing GD.



Graph 1

5. CONCLUSION

This paper thoroughly expounds the impact of Gratuitous Detour, a route malfunction exhibited by the intermediate node on the ad hoc network routing. The proposed solution buys in the idea of creating PFL and SFL backed by Dominant Pruning method. The nodes in both lists periodically handshake with each other to prune the non existent nodes and uncover the hidden nodes in the route cache of the intermediate nodes. This Intermittent Intelligent Information (I^3) provided by intermediate node augment the sender node to perform an effective network troubleshoot and diagnosis to thwart GD and thereby ensures the sustenance of network performance and throughput. A graph has been simulated to study the interdependency between the no. of misbehaving nodes and the mobility ratio of the nodes.

REFERENCES

[1] Besemann, C., Kawamura, S., and Rizzo, F., "Intrusion Detection System in Wireless Ad-Hoc Networks: Sybil Attack Detection and Others", Conference on Sensor and Ad Hoc Communications and Networks, Santa Clara, California, October 4-7, 2004.

[2] Kefayati, M., Rabiee, R.H., "Misbehavior Resilient Multi Path Data Transmission in Mobile Ad Hoc Network", *SASN'06,* October 30, 2006, Alexandria, Virginia, USA, ACM, 2006, pp. 259 – 268.

[3] Pathan, K.S.A., Alam, M., Monowar, M., and Rabbi, F., "An Efficient Routing Protocol for Mobile Ad Hoc Networks With Neighbor Awareness and Multicasting", IEEE SECON 2004

[4] Hu, C.Y., Perrig, A., "A Survey of Secure Wireless Ad hoc Routing", IEEE Computer Society, Nov.-Dec. 2006, pp. 12 – 23.

[5] Hu, C.Y., Perrig, A., Johnson, D.B., ‘‘Ariadne: A secure on-demand Routing Protocol for Wireless ad hoc networks, in the *8th Annual International Conference on Mobile Computing and Networking* September 2002 pp. 12--23.

[6] L.Zhou and Z.J.Haas, "Securing ad hoc networks" IEEE Network Magazine, 13(6): pp 24-30, November/December 1999.

[7] Babu, M.R., and Selvan, S., "Secure Source Routing Protocol for Mobile Adhoc Networks", (IJCNS) International Journal of Computer and Network Security, Vol. 2, No.7, July 2010.

[8] Yau, P.W., Hu, S., and Mitchell, C.J., "Malicious Attacks on Ad hoc Network Routing Protocols", Information Security Group.

[9] Nguyen, H.L., and Nguyen, U.T., "A Study on Different Types of Attacks on Multicast in Mobile Ad hoc Network", Ad hoc Networks (2008) pages 32-46.

[10] Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L., "Security in Mobile Ad Hoc Networks: Challenges and Solutions", UCLA Computer Science Department.

[11] Marti, S., Giuli, T.J., Lai, K., and Baker, M., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Department of Computer Science, Stanford University.

[12] Athanasiou, G., Tassiulas, L., and Yovanof, G.S., "Overcoming Misbehavior in Mobile Ad Hoc Networks: An Overview".

[13] Rabara, S.A., Vijayalakshmi, S., "Byzantine Behaviour (B2) – Mitigating Midway Multicast Misbehaviour in Adhoc Network", (IJNSA), International Journal of Network Security and Applications", Vol. 2, No.3, July 2010 pages 119-130.

[14] Iyengar, N.C.S.N., "An Efficient and Secure Routing Protocol for Mobile Ad-hoc Networks", (IJCNC), International Journal of Computer Networks and Communications", Vol. 2, No.3, May 2010, pages 28-36.

[15] Imran, N., Khan, S., Rao, I., "A Trustworthy and Well-Organized Data Disseminating Scheme for Ad hoc Networks", (IJCNC), International Journal of Computer Networks and Communications", Vol. 2, No. 3, May 2010, pages 170-181.

[16] Nakayama, H., Kurosawa, S., Jamalipour, A., "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad hoc Networks", IEEE Transactions on Vehicular Technology, Vol.58, No.5, June 2009.

[17] Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., Nemoto, Y., "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol. 5, No.3, pp 338-346, Nov 2007.

Authors

S. Vijayalakshmi is Senior Lecturer in Dept. of Computer Applications, IFET College of Engineering, Villupuram affiliated to Anna University, Chennai. She is a Ph.D candidate currently doing research work on security in ad hoc networks. She holds M.C.A degree from SR College, Bharathidasan University, Trichirapalli and M.Phil degree from Alagappa University, Karaikudi. She has a teaching experience of 6 years in the field of Computer Science. She has authored 9 research papers which are published in refereed national and international journals and conferences.

Dr.S.Albert Rabara is working as an Associate Professor in the Dept. of Computer Science, St.Joseph's College (Autonomous), (Bharathidasan University) Tiruchirappalli. He obtained his Ph.D Degree in Computer Science from Bharathidasan University. An expert in the field of Information and Communication Technology and Security, he is a consultant for several colleges in Tamil Nadu. He has 22 years of teaching and research experience and guided four Ph.D Scholars. Published more than 40 papers in Journals, International and National Conference Proceedings, his research contribution is significant in IEEE, ACM and Springer Science publications and DBLP library catalogues. He is a member of editorial board of several International Journals.