An Extension to Secure Hybrid Routing Protocol to Combat Malicious Packet Dropping in a MANET

Shirina Samreen
Research Scholar, Dept. of Computer Science
JNTUH College of Engineering
Kukatpally, Hyderabad, A.P., India

G.Narasimha, PhD.
Associate Prof., Dept. of Computer Science
JNTUH College of Engineering
Kukatpally, Hyderabad, A.P., India

ABSTRACT

Communication in a Mobile ad hoc network is accomplished in a multi-hop fashion wherein the nodes themselves act as routers as well as source. MANET is vulnerable to a variety of insider as well as outsider attacks because of it's inherent characteristics like dynamically changing topology, limited power and no centralized authority to monitor the behaviour of the nodes . Most of the secure routing protocols focus on the control plane attacks targeting the different elements of the routing protocol but data plane attacks are more difficult to handle for which we need to ensure secure data forwarding since certain adversarial nodes may launch a number of attacks on the data transmission by simply dropping the packets without forwarding them. The current paper is an extension to our earlier work where we addressed one of the most difficult data plane attacks namely, the packet dropping attack. In our earlier work, we had proposed a secure hybrid routing protocol which combats the packet dropping attack carried on by an individual / colluding adversaries and elaborated upon the first two phases of Secure Least Cost route establishment and Detection of individual node / colluding nodes maliciously dropping packets. Once a node has been identified as an adversary, we need to work upon the remedial action to prevent the future routes from involving adversarial nodes. In the current paper, we elaborate upon the last two phases namely: Punishing the adversarial nodes upon misbehaviour detection and Propagation of information about node misbehaviour and good behaviour. The current paper extends our earlier work by considering an additional colluding adversarial model consisting of consecutive nodes on the route from source to destination acting as colluding adversaries. Finally the protocol results in the establishment of a route including those nodes with good packet forwarding behaviour.

General Terms

Mobile Ad hoc Networks (MANETs), Routing Protocols, Attacks on MANET, Secure Routing.

Keywords

Colluding adversaries, Packet Drop Attack, Bloom filters, Secure Hybrid Routing Protocol.

1. INTRODUCTION

Mobile ad hoc networks are being extensively used in many distributed applications since the evolution of wireless networking and mobile computing hardware. The inherent characteristics like the infrastructure less property, ease of deployment along with self-organizing nature makes them useful for many military and disaster response applications.

On one side, certain characteristics contribute to a MANETs applicability in a number of applications, on the other side certain characteristics act as constraints for it's applicability. These characteristics include unpredictable changes in the signal strength which result in fluctuations in data transmission, mobility of nodes resulting in broken links or changed topology and the limited battery power of mobile nodes. Hence a MANET cannot be considered as an alternative to a wired network and especially the security aspect in MANET still demands a lot research because of the existence of lots of vulnerabilities which expose them to many insider as well as outsider attacks. Insider attacks come up since a MANET is based upon multi-hop packet forwarding for data transmission and outsider attacks arise due to the existence of open wireless medium.

The routing protocols designed for MANET have to take into consideration the inherent characteristics. Broadly the two approaches used are proactive routing and reactive routing. Proactive approach is table driven wherein the nodes have to work on keeping track of the routes with the changing topology irrespective or whether a route is required currently or not whereas reactive approach is an on-demand approach where route computation is done only when it is required. Each of these approaches, have their own trade-offs with respect to MANET. Proactive approach avoids delay in route establishment as routes are pre-computed but since nodes are resource-constrained in MANET, continuous maintenance of routes with changing topology puts a lot of computational burden on nodes. Reactive approach has no computational burden on nodes as routes are computed only on demand but this approach involves delay in route establishment. A hybrid approach using both proactive and reactive routing can result in higher efficiency and scalability.

Wireless networks need to operate in adversarial environments since they are prone to a number of insider as well as outsider attacks because of their inherent characteristics. Based upon the elements of the network which are effected, these attacks can be broadly categorized as control plane attacks and data plane attacks. Control plane attacks target the operation of the routing protocol and correctness of protocol messages. Data plane attacks observe violations in the forwarding decisions made by a node.

Under these circumstances, we need to design a protocol which works on security in all aspects taking into consideration the major attacks. A number of secure routing protocols are available today for mobile ad hoc networks which focus on the control plane attack and provide security against those attacks targeted upon various components of the routing protocol. To address the data plane attack, we need to have a routing protocol which ensures secure forwarding of the packets from source to destination.

One of the most challenging attacks is the packet drop attack after the establishment of secure route. The adversary simply drops the packet without forwarding them and such behaviour is referred to as byzantine behaviour. To combat the byzantine behaviour, we need a protocol which provides protection against the attacks targeting route discovery as well as data forwarding.

We design a secure routing protocol which uses a hybrid approach like the Zone routing protocol [1] [2] since it comes with advantages of both reactive and proactive approaches. To provide protection against byzantine behaviour involving malicious packet dropping, the protocol has to continuously monitor the data forwarding activity in the form of acknowledgments from the destination node. Upon the detection of packet drops, it uses a mechanism for detecting adversarial nodes on the path and assigns higher weight / cost to those nodes which will act as a metric based on which least cost route has to be formed. Hence a secure route having least cost indicates a route in which those nodes which have been detected as individual / colluding adversaries performing a packet drop are included with minimum probability. Apart from route formation, our protocol also has to take care of propagation of information about any change in any node's weight based upon it's behaviour. Since the underlying approach used by our protocol is based upon Zone routing protocol, the proactive routing tables maintained by each of the nodes whose zones include the adversarial node have to be updated with modified route costs whenever there is any change in the node's weight.

The remainder of the paper is organized as follows: Section 2 presents the related work which discusses the secure routing protocols and various approaches to detect the malicious packet dropping. Section 3 presents the design of proposed protocol with a detailed description of each of the phases and the different individual / colluding adversarial models considered. Finally section 4 presents the conclusion wherein we discuss the efficiency of the protocol.

2. RELATED WORK

Most of the routing protocols for MANETs use the number of hops as a metric to form the shortest route from source node to destination node. This metric cannot be considered as good metric for applications that focus on throughput and especially when there is a possibility of adversarial behaviour in the form of insider attacks, number of hops cannot be considered as a routing metric for secure routing.

A number of secure routing protocols have been designed for MANET which address many critical security aspects like message integrity and authentication. In [3], a protocol was proposed which guarantees minimum path selection using onion-like encryption technique and authentication is accomplished through digital signatures and public key encryption/decryption performed at each hop along the route. Other significant works include SEAD [4] and Ariadne [5] which provide secure routing through DSDV [6] and DSR [7] respectively. SEAD uses one-way hash chains and Ariadne uses TESLA [8] for authentication.

Other relevant works which focus on malicious packet dropping adversarial model are as follows:

- Credit-based techniques
- Monitoring based techniques
- Acknowledgement based techniques.

The credit based techniques by Buttyan and Hubaux [9], [10] are based upon the usage of credits called nuggets that will be awarded for a node for packet forwarding. Two models have been proposed known as Packet Purse Model and Packet Trade Model. In both these models, each intermediate node receives nuggets for packet forwarding activity which it requires for transmitting it's own data packets. Hence every node intends to increase it's nugget count for which it performs packet forwarding for other nodes. Another approach known as Sprite proposed by Zhong et al [11] uses a central server reachable through internet called Credit Clearance service which either charges or credits the nodes for packet forwarding activity depending on whether they have provided the service to others or utilized the service from others. The drawback of these techniques is that, they need tamper-resistant hardware to prevent the nodes from modifying the credit-related information.

Monitoring based techniques are based upon the promiscuous listening of neighbourhood by the wireless nodes which use the omni-propagation of wireless signals to keep track of the behaviour of their neighbours. Marti et al [12] proposed a mechanism that can be used with Dynamic source routing (DSR) protocol which includes two components namely watchdog and pathrater. The watchdog in each node monitors the behaviour of it's neighbours to see if they forward the packets to their next-hop neighbours. The information gathered by watchdog is used by the pathrater to rate the paths and the path which best avoids misbehaving nodes is chosen. Another approach called CONFIDANT [13] was proposed by Buchegger and Boudec which involves a monitor on each node keeping track of forwarding activity of neighbours and propagation of any suspicious behaviour to reputation system which rates the suspicion based on some factors. This information may further be passed on to path manager based on rating of suspicion which modifies the route cache. Finally, trust manager propagates alarm messages to all the nodes about the suspected node. Michiardi et al [14] proposed another mechanism called CORE which is a reputation based mechanism wherein reputation metrics are assigned to the nodes based upon observations made by neighbours, positive reports and task specific behaviour. The drawback of both these approaches is that, they are based upon promiscuous overhearing which is energy consuming and may raise false alarms in the presence of receiver collisions and ambiguous collisions. It may be difficult to use in multi-channel networks which use directional antennas since nodes may be engaged in parallel transmissions in orthogonal channels. The reputation mechanism can be itself exploited by colluding malicious nodes to wrongfully accuse correct nodes or increase each other's reputation by providing false observations about each other.

Acknowledgement based techniques require the nodes forwarding the data packets to send acknowledgements to their multi-hop upstream neighbours in the reverse direction of data traffic. An example of this scheme is 2ACK technique proposed by kejun Liu [15] wherein the misbehaviour is detected based upon number of packets which missed the acknowledgments. Padmanabham et al [16] proposed a technique based on traceroute wherein the source probes the route by sending pilot packets that are indistinguishable from data packets. The drawback of these techniques is that they are proactive in nature which leads to lot of network traffic created in the form of acknowledgement packets. The adversarial model considered by these techniques does not work in the presence of multiple colluding adversaries.

The ODBSR [17] (On demand byzantine resilient routing protocol) is a routing protocol which combats the colluding byzantine behaviour. It uses a reactive approach for forming routes by taking into consideration the behaviour of the nodes represented by weights assigned to each link. In other words, apart from working on the formation of routes, it works on continuous monitoring of the behaviour of nodes during data forwarding. Even though ODBSR protects against a number of byzantine attacks, since it is reactive in nature, it incurs significant delay during the route formation.

3. PROPOSED PROTOCOL

The basic idea here is once a route from source node S to destination D has been computed, the route may be secure in the sense that it protects the contents of the data packets which are being transmitted but in the presence of one or more adversaries along the route, the data transmission activity itself may not have security as these adversaries may drop the data packets without forwarding them along the route from S to D. We propose to design a secure hybrid routing protocol which is resilient to this type of malicious packet dropping by assigning weights / costs to each of the nodes based on their behavioural patterns over a period of time. The protocol provides protection against packet dropping performed by an individual node or by multiple nodes acting in collusion.

We have chosen the zone routing protocol as our base protocol since it is a hybrid routing protocol which combines the best features of both proactive and reactive approaches. To provide security to the contents of the data packets during transmission, we address major security issues like end to end authentication, packet integrity and confidentiality. For the purpose of authentication, we use RSA digital signature mechanism and for confidentiality, we use an integrated approach of both symmetric and asymmetric encryption. To provide security to the data transmission, in the presence of individual / colluding adversaries which perform malicious packet dropping, we use a mechanism of analyzing the behavioural patterns of the nodes based on which weights are assigned to the nodes and the malicious nodes are identified and their weights are adjusted accordingly to indicate their behaviour. This information has to be appropriately propagated to the remaining nodes so that these malicious nodes are given lesser preference during route formation between the source node and destination node. The value given to represent the weight of a node indicates the extent of misbehaviour. The lesser the weight of a node, the more it will be preferred during route formation. For each route, we will be computing the total cost/weight of the route and the route with minimum cost will be selected by the source.

More specifically, in terms of Zone routing protocol, both the intrazone routing protocol [18] as well as interzone routing protocol [19] have to be modified to form the routes by taking into consideration the weights of the nodes. The intrazone routing which involves proactive routing will now have routing tables with costs assigned to each of the routes and upon misbehaviour detection of a node the weights of such nodes should be modified and accordingly the total costs of the routes involving such nodes should be modified. For the interzone routing protocol, which is reactive in nature, the route computation is done dynamically by the bordercast flooding [20] of SLREQ (Secure Least Cost Route Request) packets until they reach the destination node's zone and the Secure Least Cost Route is obtained by the source node S in the form of SLREP (Secure Least Cost Response) packet.

The working of the protocol involves the following phases:

- Secure Least Cost route establishment
- Detection of individual node / colluding nodes maliciously dropping packets
- Punishing the nodes by increasing their weight proportional to the number of packets dropped
- Propagation of information about node misbehaviour and good behaviour

3.1 Secure Least Cost Route Establishment

During the Secure Least Cost route establishment phase, a secure route between the source S and the destination D is set up such that it is the least cost available route. The cost of a route is computed by taking the sum total of the costs/weights of all the nodes on the route. Initially all nodes upon entering the network have a weight zero. As networking activities of packet forwarding take place, nodes may be assigned a weight greater than zero depending upon it's behaviour over a period of time. The detailed working of this phase has been covered in our earlier work [21].

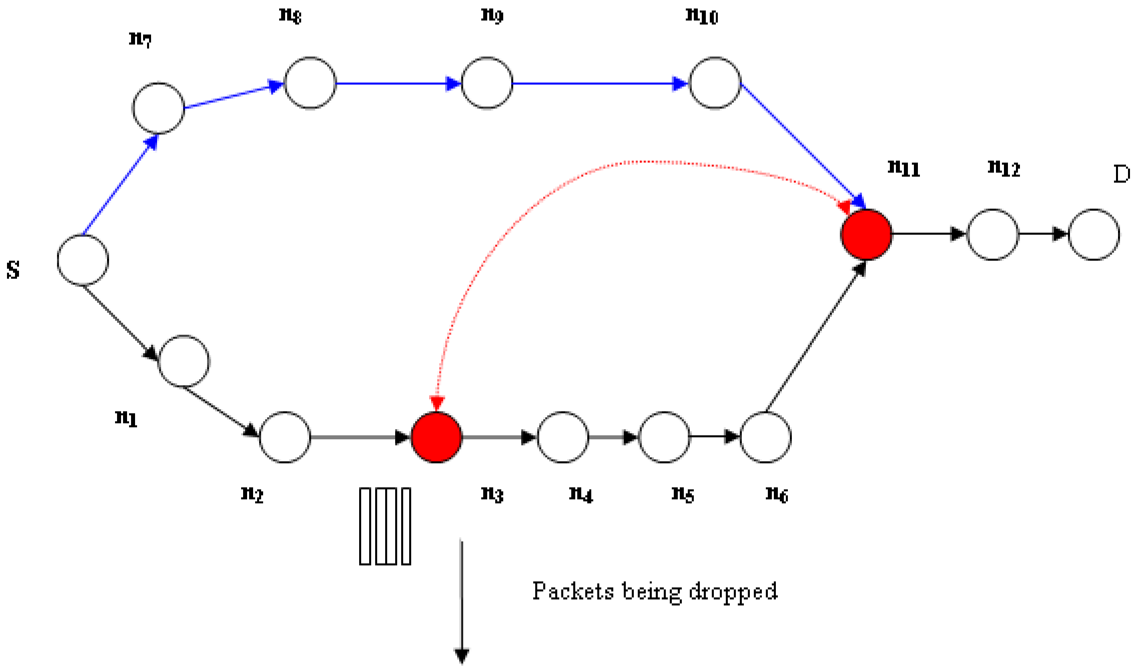
3.2 Detection of Individual / Colluding Adversaries

In our protocol, the source node has to receive an acknowledgement for every received packet by the destination node. The source buffers all the sent packets within one time window which have been transmitted. Whenever a packet misses an acknowledgment, it is considered as a packet loss which may be due to congestion at a particular node on the route or due to malicious packet dropping. We set a certain threshold indicating an acceptable amount of packet losses on a route due to congestion. When the total number of losses on a particular route crosses the threshold, the source assumes that malicious packet dropping is occurring by a single adversarial node or multiple colluding adversaries on the path. The source now enters into the phase of Detection of individual / colluding adversaries.

In this phase, the source uses bloom filters as behavioural proofs of the nodes on the path while auditing. The detection of an adversary in the adversarial model of an individual adversary and a colluding adversarial model consisting of two non-consecutive nodes as adversaries has been covered in our earlier work [21] and [22]. In the current paper, we consider a second colluding adversarial model consisting of consecutive nodes acting colluding adversaries. This phase requires the network to satisfy the following two requirements that there exists at least two node disjoint paths for every pair of nodes in the network. Also, the source knows the identity of every intermediate node on the path from S to D and a pair wise key is used to protect the communication.

3.2.1 Detection of multiple colluding adversaries- Adversarial Model 1

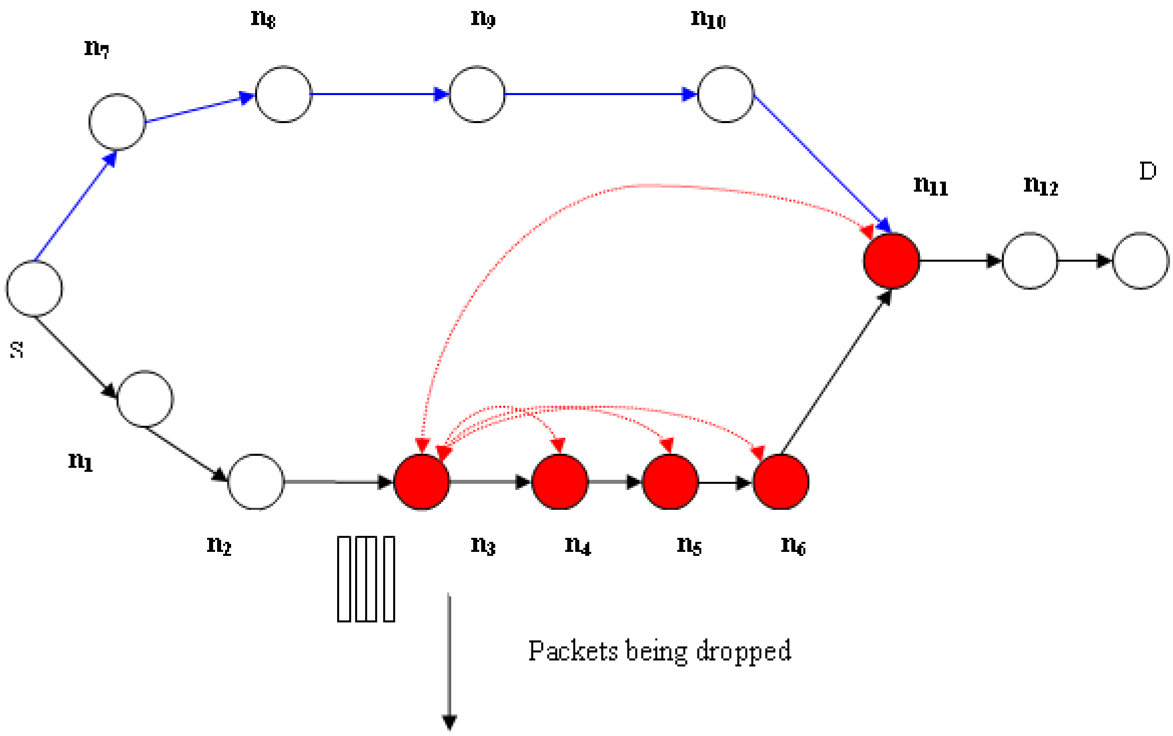
Two non-consecutive nodes ni and nk on the path from source S to destination D are colluding adversaries which are separated by non-adversarial nodes. The node n_i receives all packets from it's predecessor on the path but it drops all packets without forwarding it to it's successor on the path and hence no nodes after n_i receive any packet. If the node n_k is chosen for auditing, it will communicate with the node n_i the audit request packet specifying the sequence numbers of the packets. The node n_i generates the bloom filter and forwards it to node n_k. The node n_k sends back the bloom filter to the source S along with it's signature. If this bloom filter matches with that of source S, then S assumes that the misbehaving node is in the path segment from n_k to D. An example of the above adversarial model is as follows:



The countering of the above colluding adversarial model has been covered in our earlier work [21] and [22].

3.2.2 Detection of multiple colluding adversaries-Adversarial Model 2

A set of consecutive nodes n_i, n_{i+1}, n_{i+2},…. n_k on the path from source S to destination D are acting as colluding adversaries. In this scenario, the first node in the set receives the packets from it's predecessor node n_{i-1} in the path but it drops them without forwarding them to it's successor n_{i+1} in the path. The node n_i buffers all these packets and whenever source S sends the audit request packet to any node n_x in the set (n_{i+1}, n_{i+2}, …. n_k) on the path , the node simply communicates with node n_i the audit request packet specifying the packet sequence numbers obtained from source S. The node n_i then constructs the bloom filter and sends it to node n_x which sends it back to the source S along with it's signature. The source S verifies the received bloom filter with it's own bloom filter. If a match occurs, then S assumes that n_x has received all packets. In this way, any node n_x in the set (n_{i+1}, n_{i+2}, …. n_k) being audited will obtain the bloom filter from n_i and S assumes that misbehaving node is in the path segment from n_{x+1} to D. But the fact is, no node in the path after node n_i receives the packets since n_i drops all the packets. An example of the above adversarial model is as follows:



In the path from S to D, the nodes n_3, n_4, n_5, n_6 and n_{11} have been compromised and act as colluding adversaries. All these nodes work in cooperation to allow n_3 to perform packet dropping and also escape from being detected. No node after n_3 in the path from S to D receives any packets and if the random node chosen for auditing is any node from the set of colluding adversaries, they simply obtain the bloom filter from node n_3 and send it back to S which results in S considering the wrong path segment as suspicious.

In this case, the bloom filters of n_k as well as n_{k-1} will match S. We go for using the promiscuous listening mode which requires that each node maintains the details of the forwarding behaviour of it's neighbouring nodes. Each node maintains the information about the packets which it hears from it's neighbour by incorporating the id of the neighbour node and also the timestamp at which the packet was overheard. Whenever the random audit request packet is sent from source S, it also includes along with packet sequence numbers, the time period specified in the form of start timestamp and end timestamp during which the packets might have been received from upstream neighbours and forwarded to downstream neighbours on the path from S to D. Whenever audit request packet is sent to a node, it first generates the bloom filter which is sent to source S. If it matches, there exists a possibility of colluding attack involving consecutive neighbouring nodes. So S uses the information from neighbouring nodes about the packet overhearing statistics. If the neighbour of the node being audited reports that, no transmission is overheard within the time period as specified by audit request packet but the bloom filter matches, then that node is malicious which is getting the bloom filter from one of it's upstream neighbour which is the colluding adversary.

The modules COLL ATTCK DEFNS MODL2 and PROCESS PATHSEG are collectively used to counter this adversarial model. The working of COLL ATTCK DEFNS MODL2 is as follows: It first chooses a random node n_i in the path segment from S to D for auditing. Then it checks the bloom filters of n_i and predecessor n_{i-1}. When both of them match with the bloom filter of S, it checks for the packet overhearing statistics from the neighbourhood. If no packet overheard at n_i and n_{i-1}, then set of consecutive colluding adversaries are present upstream n_i which have to be located. This is done the module PROCESS PATHSEG. If no packet overheard at n_i but packet overheard at n_{i-1}, then nodes n_i and n_{i-1} are colluding adversaries and they are blacklisted. If packet overheard at n_i and also at n_{i-1}, then colluding adversaries are present downstream n_i and suspicious path segment is reduced to n_i -D.

The module PROCESS PATHSEG (A, B) works as follows: A random node n_i is chosen from the path segment A-B and the bloom filter is checked with that of S for a match. If it matches and according to neighbours of n_i, if no packet is overheard at n_i, then we blacklist all nodes from n_i to B as consecutive colluding adversaries. Also, there are more colluding adversaries upstream n_i and we further process the path segment from A- n_i. If bloom filter of n_i matches and also packet is overheard at node n_i, then n_i is starting node in the set of consecutive colluding adversaries.

3.3 Punishing the Adversarial Nodes upon Misbehaviour Detection

Once a node is identified as misbehaving in the form of individual / colluding adversary carrying out a packet drop attack, the node has to punished be and this is done by increasing the node's weight appropriately. The amount by which the weight has to be increased depends upon the number of packets which have been dropped by the node. For this, whenever an adversary is detected by the source, after finding a mismatch in the bloom filters of itself and that of the node being audited, the source also considers the number of bit positions which mismatch (a bit position with a 1 in the source's bloom filter and a 0 in the audit node's bloom filter) which indicates the number of packets that have been dropped by the adversarial node.

For deciding the amount by which a node's weight has to be increased upon the misbehaviour detection, we also take into consideration, the number of allowable packet losses due to congestion. Suppose, if Y represents the number of packets which may be dropped due to congestion and X represents the number of packets which have been dropped by a node. (the number of bit positions which mismatch in the source and audit node's bloom filters as 1 in source's bloom filter and a 0 in audit node's bloom filter), then the amount by which a node's weight is increased is X-Y. Since the route establishment involves the formation of least cost route, the malicious nodes will be considered for a certain route when no other alternative route is available. Hence the misbehaving nodes are penalized by reducing the probability of their involvement in the future routes. Also, we design the route establishment in such a way that, for any node, the SLREQ packet will not be forwarded further if it's weight is greater than zero. Hence a misbehaving node can neither involve in packet forwarding activity nor transmit it's data packet.

A node which is detected as an individual / colluding adversary cannot be permanently blacklisted. In order to give it a second chance for the active participation in the networking activity, whenever a node with weight greater than zero is chosen for packet forwarding because of the unavailability of alternative route, the weight is decremented by 1 for each successfully forwarded packet. In this way, we are rewarding the node under punishment for it's packet forwarding activity. Hence as the weight decreases, the probability of the node being included in a future route increases. Finally, when the weight of the node becomes zero, it becomes a normal node which can again involve in every networking activity.

3.4 Propagation of Information about Misbehaviour and Good Behaviour

A node's weight may change under two circumstances:

- Upon it's detection as an adversary which corresponds to misbehaviour
- Upon given a second chance to improve it's behaviour by involving it in packet forwarding which corresponds to good behaviour

When the source determines that a node is an individual / colluding adversary, it needs to propagate this information. More specifically, the modified weight of the node reflecting an estimate of number of packets that have been dropped has to be propagated within the network.

The information about any change in the node's weight is propagated by the source as follows: The source node bordercasts an ALARM packet containing the IP address of the adversarial node and the corresponding modified weight by signing it. This ALARM packet is further bordercasted by each of the peripheral nodes of the source and so on until the ALARM packet has reached all the zones. Duplicate ALARM packets are avoided by associating each one of them with an id. Upon receiving an ALARM packet, each node checks the id and the IP address of the source which sent the packet, to see if it had already received the packet. Upon receiving an ALARM packet, each node checks if the specified node which is an adversary falls within it's zone. If yes, then it will appropriately modify the proactive routing table entries to reflect the changed cost of each route involving the adversary.

A node which was detected as an adversary may start behaving correctly by forwarding all the packets without dropping them. As mentioned earlier, each node detected as an adversary is given a second chance by allowing them to forward packets when no alternative route is available. For each successful packet forwarding, the weight of the node is decremented by 1 and when it reaches zero, the node is considered as a normal node. After the initial route establishment phase, the source keeps track of those nodes on the route which have a weight greater than zero. During data transmission, the source node uses a mechanism wherein it has to receive an acknowledgement from the node which is downstream to that node on the route which had a weight greater than zero during the initial route establishment. In this mechanism, with each data packet which is transmitted the source node specifies the IP address of those nodes from which it expects an acknowledgment (upstream neighbours of those nodes with weight greater than zero). For each such received acknowledgement, the source node checks the node which is upstream to the sender of the acknowledgement and decrements it's weight by 1. When the weight becomes zero, the source takes charge of propagating the modified weight of the node in the form of ALARM packet so that the proactive routing tables of all the zones to which the node belongs can be updated accordingly.

4. CONCLUSION

Our proposed routing protocol uses a mechanism which forms routes by avoiding those nodes which have been detected as being malicious packet droppers in the past. At the same time, nodes detected as misbehaving are given a second chance to improve their behaviour. Since the underlying routing protocol is the hybrid Zone routing protocol, it is efficient in terms of route formation as it exploits the benefits of both proactive and reactive approaches. We plan to simulate our proposed protocol using ns-2 network simulator and analyze its performance and efficiency in the presence of individual adversarial model and the two different colluding adversarial models which result in maliciously dropping the packets.

5. REFERENCES

[1] Haas Z. J., Pearlman M. R., and Samar P., "The Zone Routing Protocol (ZRP)", IETF Internet Draft, draft-ietf-manet-zone-zrp-04.txt, July 2002.

[2] Jan Schaumann, "Analysis of Zone Routing Protocol", Course CS765, Stevens Institute of Technology Hoboken, New Jersey, USA, 8th December 2002

[3] Sanzgiri, Dahill, Levine, Shields and Belding-Royer, "A secure routing protocol for ad hoc networks," In Proceedings of IEEE International Conference on Network Protocols (ICNP). 2002.

[4] Hu, Y., Johnson, and Perrig, "SEAD: Secure Efficient Distance Vector Routing For Mobile Wireless Ad Hoc Networks," In Proceedings Of IEEE Workshop On Mobile Computing Systems And Applications (WMCSA). 2002

[5] Hu Y., Perrig, and Johnson, "Ariadne: A Secure On-Demand Routing Protocol For Ad Hoc Networks," In Proceedings Of ACM Annual International Conference Of Mobile Computing (MOBICOM).

[6] Perkins, C. E. And Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) For Mobile Computers," In Proceedings Of

SIGCOMM Conference On Applications, Technologies, Architectures, And Protocols For Computer Communication (SIGCOMM).1994

[7] Johnson, Maltz, And Broch, "DSR: The Dynamic Source Routing Protocol For Multi-Hop Wireless Ad Hoc Networks." In Ad Hoc Networking. Addison-Wesley, Chapter 5, 139–172.

[8] Perrig, Canetti, Song, And Tygar, "Efficient And Secure Source Authentication For Multicast," In Proceedings Of ISOC Symposium Of Network And Distributed Systems Security (NDSS).

[9] L. Buttyán, and J. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," Mobile Net works and Applications, 8(5), pp. 579-592, 2003.

[10] M. Jakobsson, J.-P. Hubaux, and L. Buttyan, "A micropayment scheme encouraging collaboration in multi-hop cellular networks," in Financial Crypto, 2003.

[11] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple cheat-proof, credit-based system for mobile ad-hoc networks," in IEEE INFOCOM, pp. 1987-1997, 2003.

[12] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proceedings of the 6th Annual international Conference on Mobile Computing and Networking (MOBICOM), pp. 255-265, 2000.

[13] S. Buchegger and J.-Y. L. Boudec, "Self-policing mobile ad-hoc networks by reputation systems," IEEE communications Magazine, pp. 101-107, 2005.

[14] P. Michiardi, and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in Proceedings of IFIP Joint Working Conference on Communications and Multimedia Security, pp.107-121, 2002.

[15] K. Liu, J. Deng, P. Varshney, K. Balakrishnan, "An Acknowledgment Based Approach for the Detection of Routing Misbehavior in MANETs," IEEE Transactions on Mobile Computing, 6(5), pp. 536550, 2007.

[16] V. Padmanabhan, D. Simon, "Secure traceroute to detect faulty or malicious routing," ACM SIGCOMM Computer Communication Review, 33(1), pp. 77-82, 2003.

[17] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure Byzantine resilient routing protocol for wireless ad hoc networks," ACM Trans. Inf. Syst. Secur. 10(4), 1-35, 2008.

[18] Haas, Zygmunt J., Pearlman, Marc R., Samar, P.: "Intrazone Routing Protocol (IARP)", IETF Internet Draft, draft-ietf-manet-iarp-01.txt, June 2001

[19] Haas, Zygmunt J., Pearlman, Marc R., Samar, P.: "Interzone Routing Protocol (IERP)", IETF Internet Draft, draft-ietf-manet-ierp-01.txt, June 2001.

[20] Haas, Zygmunt J., Pearlman, Marc R., Samar, P.: "The Bordercast Resolution Protocol (BRP) for Ad Hoc Networks", IETF Internet Draft, draft-ietf-manet-brp01.txt, June 2001

[21] Shirina Samreen and Dr. G. Narasimha, "A secure Hybrid Routing Protocol to Combat Malicious Packet Dropping in a MANET," International Journal of Computer Applications (IJCA) Vol. 65-No.10, March 2013, ISSN: 0975-8887

[22] Shirina Samreen and Dr. G. Narasimha, "Detection of Colluding Adversaries in a Packet Drop Attack on MANET," International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 9, November- 2012 ISSN:2278-0181