Secure On Demand Multicast Routing Protocol for Mobile Ad-Hoc Networks

Saranya L.[*], T.Parameswaran[**]

[*]Final year ME (CSE) Student, Anna University of Technology, Coimbatore, Tamilnadu, India
[**]Asst.Professor, Dept of CSE, Anna university of Technology, Coimbatore

Abstract- Wireless ad-hoc networks emerged as a promising technology that offers low-cost high-bandwidth community wireless services. A WAN consists of a set of stationary wireless routers that form a multi hop backbone, and a set of mobile clients that communicate via the wireless backbone. Many applications can benefit from the service provided by multicast routing protocols. In a typical high-throughput multicast protocol, nodes periodically send probes to their neighbours to measure the quality of their adjacent links. During route discovery, a node estimates the cost of the path by combining its own measured metric of adjacent links with the path cost accumulated on the route discovery packet. The path with the best metric is then selected. ODMRP, as it is a ad-hoc based protocol, which has the potential to be more attack resilient. We focus on the SPP metric based on the well known ETX unicast metric. We identify a class of severe attacks against multicast protocols that exploit the use of high-throughput metrics, including local metric manipulation (LMM) and global metric manipulation (GMM). We propose a secure high-throughput multicast protocol S-ODMRP that incorporates a novel defense scheme Rate Guard. Rate Guard combines measurement-based detection and accusation-based reaction techniques to address the metric manipulation and packet dropping attaciks.Sybil attack detection, Detection Algorithm is used to detect the Sybil attack. And individual nodes that wish to detect Sybil attackers monitor all transmissions We receive over many time intervals. These intervals are chosen long enough to capture behaviour from all the Sybil identities of an attacker, including data transmissions, HELLO and keep-alive messages, and routing requests and replies. The node keeps track of the different identities heard during the interval. Having made many observations, the node analyzes the data to find identities that appear together often and that appear apart rarely. These identities likely comprise a Sybil attack.

Index Terms- Mobile Ad-Hoc networks, high-throughput metrics, secure multicast routing, metric manipulation attacks, Byzantine attacks, Sybil attacks.

I. INTRODUCTION

A wireless Ad-Hoc network often has a more planned configuration, and may be deployed to provide dynamic and cost effective connectivity over a certain geographic area. An ad-hoc network, on the other hand, is formed ad hoc when wireless devices come within communication range of each other. The mesh routers may be mobile, and be moved according to specific demands arising in the network. Often the mesh routers are not limited in terms of resources compared to other nodes in the network and thus can be exploited to perform more resource intensive functions.

Multicast routing protocols deliver data from a source to multiple destinations organized in a multicast group. In the last few years, several protocols were proposed to provide multicast services for multihop wireless networks. These protocols were proposed for mobile ad hoc networks (MANETs), focusing primarily on network connectivity and using the number of hops (or hop count) as the route selection metric. However, it has been shown that using hop count as routing metric can result in selecting links with poor quality on the path, negatively impacting the path throughput.

Numerous protocols exist for forming ad hoc networks among cooperative mobile, radio-equipped nodes. Many ad hoc routing protocols have been secured using reputation schemes or threshold security schemes that rely on there being a limited number of attackers in the group and that assume each radio represents a different individual. However, the broad cast nature of radio allows a single node to pretend to be many nodes simultaneously by using many different addresses while transmitting.

II. HIGH-THROUGHPUT MULTICAST ROUTING

We consider a multihop wireless network where nodes participate in the data forwarding process for other nodes.We assume a mesh-based multicast routing protocol, which maintains a mesh connecting multicast sources and receivers. Path selection is performed based on a metric designed to maximize throughput. Below, we provide an overview of high-throughput metrics for multicast, then describe in details how such metrics are integrated with mesh-based multicast protocols.

2.1 High-Throughput Metrics

ETX metric: The ETX metric [10] was proposed for unicast and estimates the expected number of transmissions needed to successfully deliver a unicast packet over a link, including retransmissions. Each node periodically broadcasts probe packets which include the number of probe packets received from each of its neighbors over a time interval. A pair of neighboring nodes, A and B, estimate the quality of the link A $A \rightarrow$ B by using the formula $ETX = 1/(df * dr)$, where *df* and *dr* are the probabilities that a packet is sent successfully from A to B (forward direction) and from B to A (reverse direction), respectively. The value of ETX for a path of k links between a source S and a receiver R is $ETX_{S \rightarrow R} = ETX$ Pki¼1 ETXi, where ETXi is the ETX value of the ith link on the path; $ETX_{S \rightarrow R}$ estimates the total number of transmissions by all nodes on the path to deliver a packet from a source to a receiver.

SPP metric: ETX was adapted to the multicast setting by Roy et al. in the form of the SPP metric [11]. The value of SPP for a path of k links between a source S and a receiver R is $SPP_{S \rightarrow R} = \pi_{i=1}^{k} SPPi$, where the metric for each link i on the path is SPP_i = df and *df* is defined as in ETX. The rationale for defining SPP as above is twofold:

Unlike in unicast, where a successful transmission over a link depends on the quality of both directions of that link, in multicast only the quality of the forward direction matters because there are no link layer acknowledgments. The quality of a link A → B, as perceived by node B, is $SPP_{i \rightarrow df}$ and represents the probability that B receives a packet successfully from A over the link A → B. Node B obtains *df* by counting the probes received from A over a fixed time interval.

Also unlike unicast, in which the individual link metrics are summed, in multicast they are multiplied.This reflects the fact that for SPP the probability of a packet being delivered over a path from a source to a receiver is the product of the probabilities that the packet is successfully delivered to each of the intermediate nodes on the path. If any of the intermediate nodes fails to receive the packet, this causes the transmission for the entire route to fail, since there are no retransmissions. $SPP_{S \rightarrow R}$ (in fact $1=SPP_{S \rightarrow R}$) estimates the expected number of transmissions needed at the source to successfully deliver a packet from a source to a receiver.

SPP takes values in the interval [0 1], with higher metric values being better. In particular, SPP → 1 denotes perfect reliability, while SPP → 0 denotes complete unreliability.

2.3 High-Throughput Mesh-Based Multicast Routing

ODMRP protocol using a high-throughput metric as ODMRP-HT in order to distinguish it from the original ODMRP [6] protocol.

ODMRP overview: ODMRP is an on-demand multicast routing protocol for multi hop wireless networks, which uses a mesh of nodes for each multicast group. Nodes are added to the mesh through a route selection and activation protocol.

The source periodically recreates the mesh by flooding a JOIN QUERY message in the network in order to refresh the membership information and update the routes. We use the term round to denote the interval between two consecutive mesh creation events. JOIN QUERY messages are flooded using a basic flood suppression mechanism, in which nodes only process the first received copy of a flooded message. When a receiver node gets a JOIN QUERY message, it activates the path from itself to the source by constructing and broadcasting a JOIN REPLY message that contains entries for each multicast group it wants to join; each entry has a next hop field filled with the corresponding upstream node. When an intermediate node receives a JOIN REPLY message, it knows whether it is on the path to the source or not, by checking if the next hop field of any of the entries in the message matches its own identifier. If so, it makes itself a node part of the mesh (the FORWARDING GROUP) and creates and broadcasts a new JOIN REPLY built upon the matched entries.

Once the JOIN REPLY messages reach the source, the multicast receivers become connected to the source through a mesh of nodes (the FORWARDING GROUP) which ensures the delivery of multicast data. While a node is in the FORWARDING GROUP, it rebroadcasts any non duplicate multicast data packets that it receives. ODMRP takes a “soft state” approach in that nodes put a minimal effort to maintain the mesh. To leave the multicast group, receiver nodes are not required to explicitly send any message, instead they do not reply to JOIN QUERY messages. Also, a node’s participation in the FORWARDING GROUP expires if its forwarding node status is not updated.

ODMRP-HT: We now describe ODMRP-HT, a protocol that enhances ODMRP with high-throughput metrics. The main differences between ODMRP-HT and ODMRP are: 1) instead of selecting routes based on minimum delay (which results in choosing the fastest routes), ODMRP-HT selects routes based on a link-quality metric, and 2) ODMRP-HT uses a weighted flood suppression mechanism to flood JOIN QUERY messages instead of using a basic flood suppression.

III. Attacks Against High Throughput Multicast

3.1 Metric Manipulation Attacks

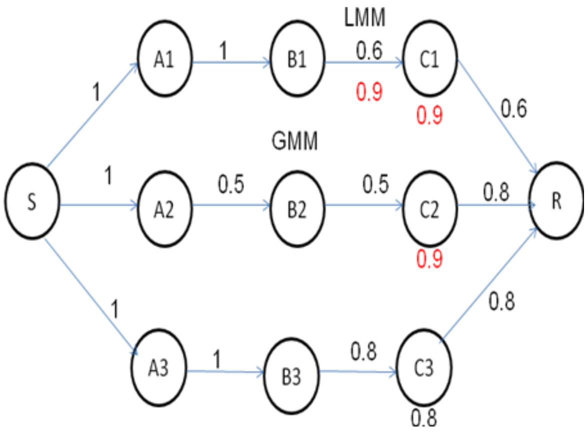


Fig.1Metric Manipulation Attack

As discussed in Section 2, multicast protocols using high throughput metrics prefer paths to the source that are perceived as having high quality, while trying to avoid low quality paths. Thus, a good strategy for an attacker to increase its chances of being selected in the FORWARDING GROUP is to advertise artificially good metrics for routes to the source. The use of high throughput metrics requires each node to collect local information about its adjacent links based on periodic probes from its neighbors. This local information is accumulated in JOIN QUERY packets and propagated in the network, allowing nodes to obtain global information about the quality of the routes from the source. Adversaries can execute two types of metric manipulation attacks: local metric manipulation (LMM) and global metric manipulation (GMM). These attacks are Byzantine in nature, as they are conducted by nodes that have the credentials to participate in the routing protocol, but are under adversarial control.

LMM attacks: An adversarial node artificially increases the quality of its adjacent links, distorting the neighbors'perception about these links. The falsely advertised "highquality" links will be preferred and malicious nodes have better chances to be included on routes. A node can claim a false value for the quality of the links toward itself. In Fig. 1, a malicious node C1 claims that SPPB1→C1=0.9 instead of the correct metric of 0.6. Thus, C1accumulates a false local metric for the link B1 −→ C1 and advertises to R the metric SPPS→C1 = 0.9 instead of the correct metric SPPS→C1 = 0.6. The route S-A1-B1-C1-R willbe chosen over the correct route S-A3-B3-C3-R.

GMM attacks: In a GMM attack, a malicious node arbitrarily changes the value of the route metric accumulated in the flood packet, before rebroadcasting this packet. A GMM attack allows a node to manipulate not only its own contribution to the path metric, but also the contributions of previous nodes that were accumulated in the path metric. For example, in Fig. 1, attacker C2 should advertise a route metric of 0.25, but instead advertises a route metric of 0.9 to node R. This causes the route S-A2-B2-C2-R to be selected over the correct route S-A3-B3-C3-R.

IV. SECURE HIGH-THROUGHPUT MULTICAST ROUTING

In this section, we present our secure multicast routing protocols-ODMRP, with a novel defence scheme RateGuard to accommodate high-throughput metrics.

4.1 S-ODMRP Overview

S-ODMRP ensures the delivery of data from the source to the multicast receivers even in the presence of Byzantine attackers, as long as the receivers are reachable through non adversarial paths. To achieve this, S ODMRP uses a combination of authentication and rate limiting techniques against resource consumption attacks and a novel technique, RateGuard, against the more challenging packet dropping and mesh structure attacks, including metric manipulations and JOIN REPLY dropping. S-ODMRP uses source message authentication to avoid processing non authenticated messages. This eliminates a large class of attacks, including outsider attacks, message spoofing and modification attacks targeting JOIN QUERY and JOIN REPLY messages, and the injection of corrupted data packets. Even with message authentication, an insider attacker can still mount the resource consumption attack by flooding JOIN QUERY messages frequently with itself as the source. Such an attack can be countered by rate limiting, for example, a honest node only forwards JOIN QUERY messages for a source node up to a maximum frequency.

To address the resource consumption attack in which the attacker activates many unnecessary data delivery paths by injecting many JOIN REPLY messages, we can limit to at most one the number of JOIN REPLY messages a node may send in one round. Each node monitors the number of different signed JOIN REPLY messages that originate from its neighbors. If a node is observed to have broadcast two or more different signed JOIN REPLY messages, then punitive actions can be taken against the node (e.g., isolation).The attacks on the mesh structure and packet dropping attacks are much more challenging to defend against, particularly, in the context of high throughput metrics. In the following, we focus on defending against these attacks. We will first present the high-level overview of our defense scheme, RateGuard, and then present the details of S-ODMRP with the RateGuard scheme.

RateGuard Overview:

RateGuard relies on the observation that regardless of the attack strategy, either by dropping JOIN REPLY, metric manipulations, or by dropping packets, attackers do not affect the multicast protocol unless they cause a drop in the packet delivery ratio (PDR). We adopt a reactive approach in which attacker nodes are detected through a measurement- based detection protocol component, and then isolated through an accusation-based reaction protocol component. Next, we describe these two components.

Measurement-based attack detection:

Whether by packet dropping alone or by combining it with metric manipulation to attract routes, the effect of an attack is that data are not delivered at a rate consistent with the advertised path quality. We propose a generic attack detection strategy that relies on the ability of honest nodes to detect the discrepancy between the expected PDR (ePDR) and the perceived PDR (pPDR). A node can estimate the ePDR of a route from the value of the metric for that route 3 the node can determine the pPDR for a route by measuring the rate at which it receives data packets from its upstream on that route.4 Both FORWARDING GROUP nodes and receiver nodes monitor the pPDR of their upstream node. If ePDR _ pPDR for a route becomes larger than a detection threshold , then nodes suspect that the route is under attack because the route failed to deliver data at a rate consistent with its claimed quality

Accusation-based attack reaction:

We use a controlled accusation mechanism in which a node, on detecting malicious behaviour, temporarily accuses the suspected node by flooding in the network an ACCUSATION message containing its own identity (the accuser node) and the identity of the accused node, as well as the duration of the accusation. As long as the accusation is valid, metrics advertised by an accused node will be ignored and the node will not be selected as part of the FORWARDING GROUP. This strategy also successfully handles attacks against path establishment. From the downstream node point of view, the dropping of a JOIN REPLY message causes exactly the same effect as the attacker dropping all data packets, thus the downstream nodes will react and accuse the attacker.

To prevent the abuse of the accusation mechanism by attackers, a node is not allowed to issue a new accusation before its previously issued accusation expires. Accused nodes can still act as receivers even though they are excluded from the

FORWARDING GROUP. We use a temporary accusation strategy to cope with transient network variations: The accusation duration is calculated proportional to the observed discrepancy between ePDR and pPDR, so that accusations caused by metric inflation and malicious data dropping last longer, while accusations caused by transient network variations last shorter. Finally, to address the metric poisoning effect caused by metric manipulation attacks, the metric in the entire network is refreshed shortly after attack detection. In SODMRP, the metric refreshment is achieved automatically through the periodic JOIN QUERY messages.

V. Sybil Attacks in Ad hoc Networks

An ad hoc network is composed of mobile, wireless de vices, referred to as nodes that communicate only over a shared broadcast channel. An advantage of such a network is that no fixed infrastructure is required: a network for routing data can be formed from whatever nodes are available. Nodes forward messages for each other to provide connectivity to nodes outside direct broadcast range.

In unsecured routing protocols, such as DSR or AODV, these address-based identifiers can be easily falsified by malicious nodes,which presents an opportunity for a Sybil attack. However, allowing unauthenticated address presents a series of other attacks, including route direction, spoofing, and error fabrication. Our methods work whether addresses are authenticated or not, though given the wide range of attacks possible against unauthenticated networks, Sybil attacks may not be the most significant problem present. Our methods will also work on disruption tolerant networks (e.g., [6]), however, just as such networks incur an extreme routing delay, there will be a corresponding large delay in successful sybil attack detection.

Secured ad hoc networks can be classified into three broad groups, each of which can be susceptible to the Sybil attack.

Threshold-based protocols: To avoid the untenable requirement of a PKI, other protocols use threshold cryptography. In such scheme, a group of trusted nodes distributes cryptographic material only if a sub set of that group agrees on the trustworthiness of new members [16, 32, 15]. Sybil attackers can additionally defeat schemes that rely on threshold cryptography because verifying the true number and independence of nodes in the network is difficult. If a Sybil attacker can generate identities to meet the threshold requirements it can effectively control the routing of the network.

5.1 Detection Protocol:

In this section, we describe two versions of our first detection protocol: a single observer case and a multi-observer case.

In the next section, we evaluate both of these proto cols. In Section 5, we show how these basic methods can be extended to include information from the MAC network layer.

After a period of observation, the detection algorithm then works in a series of simple steps:

1. We calculate Aij, the affinity between nodes i and j,

$$Aij = (Tij - 2Lij) * [(Tij + Lij)/N]$$

where Tij is the number of intervals in which nodes i and j were observed together, Lij is the number of intervals in which either i or j were observed alone, and N is total number of intervals in the observation period.

2. After the affinity between each pair of nodes has been computed, the observer constructs a graph in which the node identities are the vertices and the undirected edges are weighted with the affinity values between them. Only edges that are greater than a specific threshold parameter are included. Using our measure of affinity, we recorded our results using a threshold of 0.1.

3. Depth-first search (DFS) is then run over each vertex to discover the connected components. Each of the components found represents a possible Sybil attacker. we took only the largest to be a Sybil attacker, in line with the working assumption that there was only one per network. If there were more, they would appear as separate components.

VI. EXPERIMENTAL EVALUATION

DONG ET AL.: SECURE HIGH-THROUGHPUT MULTICAST ROUTING IN WIRELESS MESH NETWORKS 665

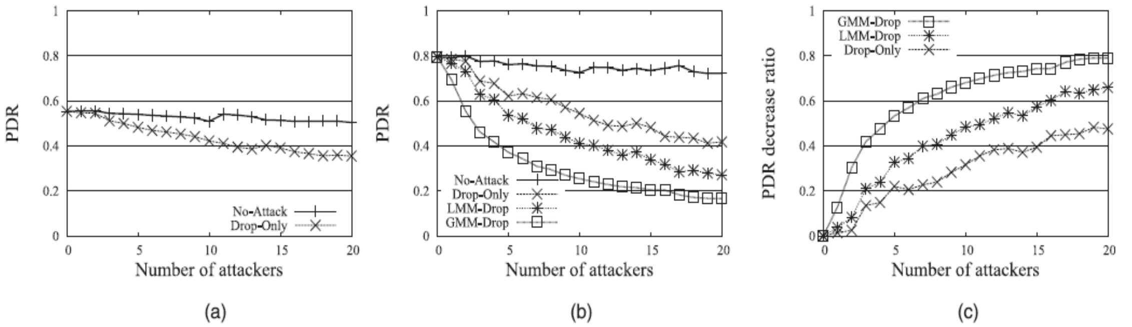
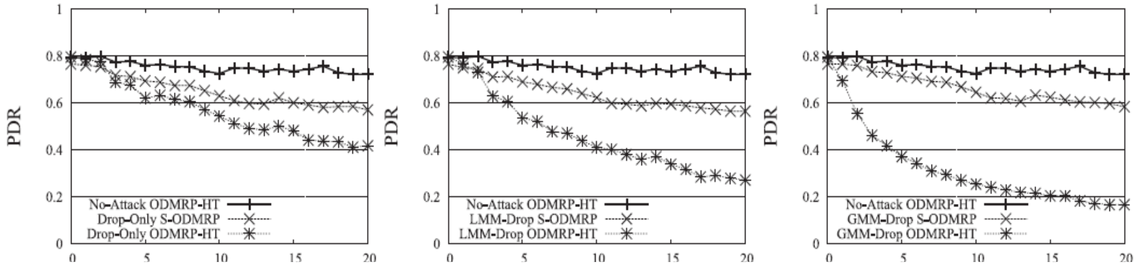
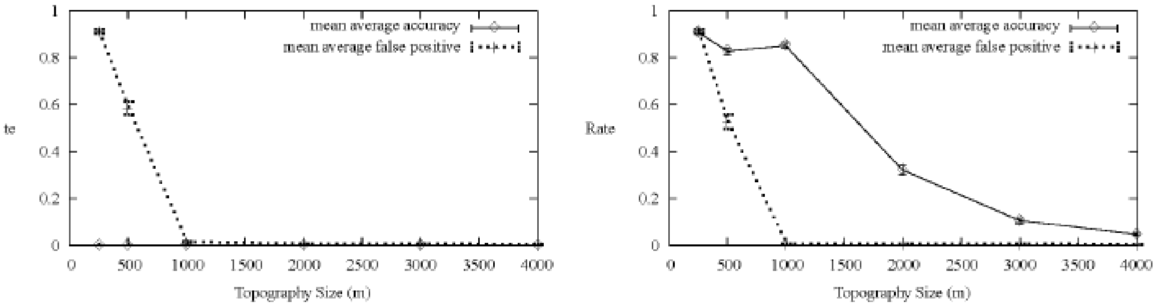


Fig. 7. The effectiveness of metric attacks on ODMRP-HT. For comparison, we include attacks against ODMRP without high-throughput metrics. (a) Attacks on ODMRP. (b) Attacks on ODMRP-HT. (c) Attack strength against ODMRP-HT.



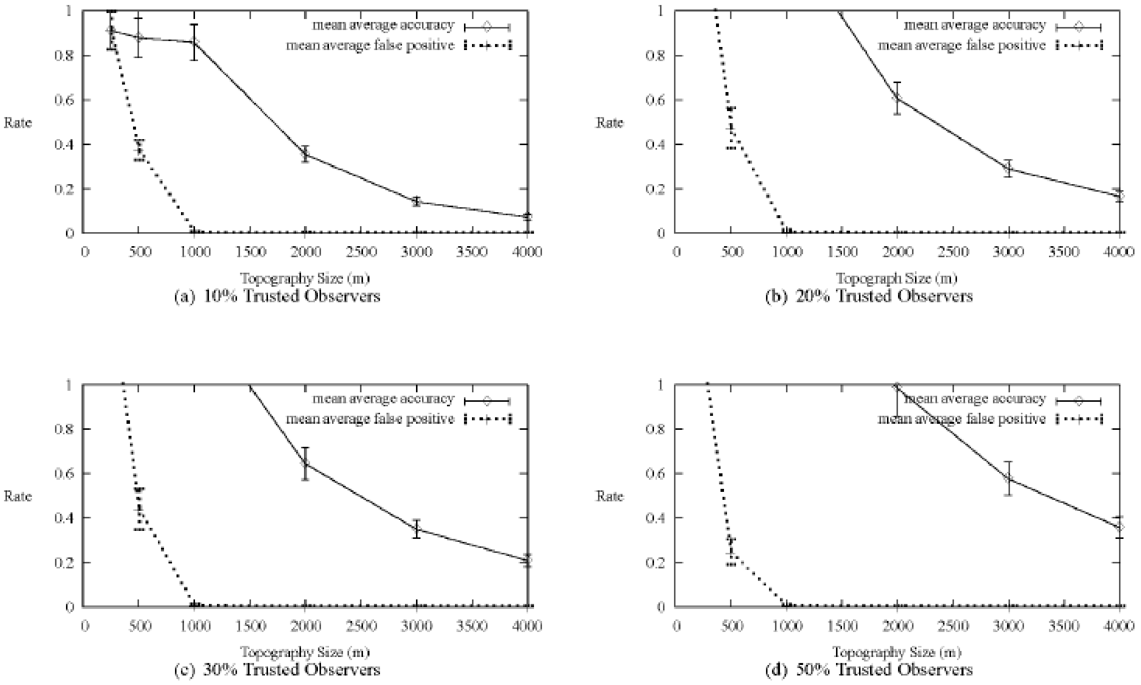
SYBIL ATTACK:



(a) No Sybil attacker present

(b) Single Sybil attacker present

Figure 1: Accuracy rates vs. topography size for a single observer



(a) 10% Trusted Observers

(b) 20% Trusted Observers

(c) 30% Trusted Observers

(d) 50% Trusted Observers

Figure 2: Accuracy rates for various percentages of observers

VII. CONCLUSION

We considered the security implication of using high throughput metrics in multicast protocols in wireless mesh networks. In particular, we identified metric manipulation attacks that can inflict significant damage on the network. The attacks not only have a direct impact on the multicast service, but also raise additional challenges in defending against them due to their metric poisoning effect. We overcome the challenges with our novel defense scheme, RateGuard, that combines measurement-based attack detection and accusation-based reaction. implementation of new technique to detect the Sybil attack in wireless mesh networks. Here we show that mobility of nodes in a wireless network can be used to detect and identify nodes that are part of a Sybil attack. And individual nodes that wish to detect Sybil attackers monitor all transmissions they receive over many time intervals. These intervals are chosen long enough to capture behaviour from all the Sybil identities of an attacker, including data transmissions, HELLO and keep-alive messages, and routing requests and replies. The node keeps track of the different identities heard during the interval. Having made many observations, the node analyzes the data to find identities that appear together often and that appear apart rarely. These identities likely comprise a Sybil attack.

7.2 Future Enhancement

The Metric manipulation attack and Sybil attack is identified in the proposed work to enhance throughput. Hence this work can be extended to find other attacks possible with this type of network and thereby increasing throughput as well as reducing packet drop ratio.

REFERENCES

[1] J. Dong, R. Curtmola, and C. Nita-Rotaru, “On the Pitfalls of Using High-Throughput Multicast Metrics in Adversarial Wireless Mesh Networks,” Proc. Fifth Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON ’08), 2008.

[2] Y.B. Ko and N.H. Aveda, “Flooding-Based Geocasting Protocols for Mobile Ad Hoc Networks,” Mobile Networks and Applications, vol. 7, no. 6, pp. 471-480, 2002.

[3] R. Chandra, V. Ramasubramanian, and K. Birman, “Anonymous Gossip: Improving Multicast Reliability in Mobile Ad-Hoc Networks,” Proc. 21st IEEE Int’l Conf. Distributed Computing Systems (ICDCS ’01), 2001.

[4] Y.-B. Ko and N.H. Vaidya, “GeoTORA: A Protocol for Geocasting in Mobile Ad Hoc Networks,” Proc. Int’l Conf. Network Protocols (ICNP), pp. 240-250, 2000.

[5] E.L. Madruga and J.J. Garcia-Luna-Aceves, “Scalable Multicasting: the Core-Assisted Mesh Protocol,” Mobile Networks and Applications, vol. 6, no. 2, pp. 151-165, 2001.

[6] S.J. Lee, W. Su, and M. Gerla, “On-Demand Multicast Routing Protocol in Multihop Wireless Mobile Networks,” Mobile Networks and Applications, vol. 7, no. 6, pp. 441-453, 2002.

[7] E.M. Royer and C.E. Perkins, “Multicast Ad-Hoc On-Demand Distance Vector (MAODV) Routing,” Internet Draft, July 2000.

[8] .G. Jetcheva and D.B. Johnson, “Adaptive Demand-Driven Multicast Routing in Multi-Hop Wireless Ad Hoc Networks,” Proc. ACM MobiHoc, 2001.

[9] H. Lundgren, E. Nordstrom, and C. Tschudin, “Coping with Communication Gray Zones in IEEE 802.11b Based Ad Hoc Networks,” Proc. Fifth ACM Int’l Workshop Wireless Mobile Multimedia (WOWMOM ’02), 2002.

[10] D.S.J.D. Couto, D. Aguayo, J.C. Bicket, and R. Morris, “A High-Throughput Path Metric for Multi-Hop Wireless Routing,” Proc. ACM MobiCom, 2003.

[11] S. Roy, D. Koutsonikolas, S. Das, and C. Hu, “High-Throughput Multicast Routing Metrics in Wireless Mesh Networks,” Proc.26th IEEE Int’l Conf. Distributed Computing Systems (ICDCS), 2006.

[12] A. Chen, D. Lee, G. Chandrasekaran, and P. Sinha, “HIMAC: High Throughput MAC Layer Multicasting in Wireless Networks,” Proc. IEEE Int’l Conf. Mobile Adhoc and Sensor Systems (MASS ’06), 2006.

[13] B. Awerbuch, D. Holmer, and H. Rubens, “The Medium Time Metric: High Throughput Route Selection in Multirate Ad Hoc Wireless Networks,” Mobile Networks and Applications, Special Issue on Internet Wireless Access: 802.11 and Beyond, vol. 11, no. 2, pp. 253-266, 2005.

[14] A. Adya, P. Bahl, J. Padhye, A. Wolman, and L. Zhou, “A Multi- Radio Unification Protocol for IEEE 802.11 Wireless Networks,” Proc. First Int’l Conf. Broadband Networks (BroadNets ’04), 2004.

[15] S. Keshav, “A Control-Theoretic Approach to Flow Control,” Proc. ACM SIGCOMM, 1993.

[16] R. Draves, J. Padhye, and B. Zill, “Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks,” Proc. ACM MobiCom, 2004.

[17] P. Papadimitratos and Z. Haas, “Secure Routing for Mobile Ad Hoc Networks,” Proc. SCS Comm. Networks and Distributed Systems Modeling and Simulation Conf. (CNDS), pp. 27-31, Jan. 2002.

[18] Y.-C. Hu, D.B. Johnson, and A. Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks,” Proc. Fourth IEEE Workshop Mobile Computing Systems and Applications (WMCSA), 2002.

[19] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, and E. Belding-Royer, “A Secure Routing Protocol for Ad Hoc Networks,” Proc. 10th IEEE Int’l Conf. Network Protocols (ICNP), 2002.

[20] S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” Proc. ACM MobiCom, Aug. 2000.

AUTHORS

First Author – Saranya.L, Final year ME (CSE) Student, Anna University of Technology, Coimbatore, Tamilnadu, India., lakssaya@gmail.com, 9894097746

Second Author – T.Parameswaran, Asst.Professor, Dept of CSE, Anna university of Technology, Coimbatore