Secluding RSGM Protocol against Multicast Attacks

A. Amuthan
Associate professor
Department of CSE
Pondicherry Engineering College, Puducherry, India

S. Parthiban
Senior Technical Assistant
Department of CSE
Pondicherry University
Puducherry, India

R.Kaviarasan
Assistant Professor
Department of CSE
Alpha College of Engg & Tech
Puducherry, India

ABSTRACT
In the presence of malicious nodes, one of the main challenges in MANETs is to design a novel, scalable and robust Geographic Multicast Protocol (RSGM) that can protect MANETs from various routing attacks. The vulnerabilities in the RSGM protocol were explored and various attacks like blackhole, wormhole and flooding attack are simulated. Several virtual architectures are used in the protocol without need of maintaining state information for more robust and scalable membership management and packet forwarding in the presence of high network dynamics due to unstable wireless channels and node movements. Specifically, scalable and efficient group membership management is performed through a virtual-zone-based structure, and the location service for group members is integrated with the membership management. Both the control messages and data packets are forwarded along efficient tree-like paths, but there is no need to explicitly create and actively maintain a tree structure. The stateless virtual tree-based structures significantly reduce the tree management overhead, support more efficient transmissions, and make the transmissions much more robust to dynamics. Geographic forwarding is used to achieve scalability and robustness. Differences mechanisms have been proposed using various techniques to countermeasure the routing attack against MANETs. However, these mechanisms are not suitable for MANETs resource constraints. In a mobile scenario, mesh based protocols outperformed tree-based protocols. The availability of alternate routes provided robustness and scalability. The different routing attacks, such as flooding, blackhole and wormhole are simulated using NS2.28 version and efficient proactive counter measure is provided using HMAC function which would lead to a drastic change is performance metric like packet delivery ratio, control overhead and end to end delay which is used to prove that the proposed solution was efficient and robust.

Keywords
Blackhole attack, Wormhole attack, Flooding attack, RSGM.

1. INTRODUCTION
A Mobile Ad-Hoc NETwork (MANET) is a collection of wireless mobile nodes forming a temporary network without using any centralized access point, infrastructure, or centralized administration. A MANET, due to its unique infrastructure less characteristic compared to other types of wireless networks, can be very useful for many applications in which no infrastructure exists. Establishing communication among a group of soldiers in a battlefield is a good example. A fixed infrastructure in enemy territories or in hostile terrains may not be possible. In such environments, MANETs [1] can provide the required communication. In addition, applications in this area requires a *secure* communication as eavesdropping or other security threats can compromise the network and threaten the safety of personnel involved in these military operations. Secure *multicast* may also be required. For example, the leader of a group of soldiers may want to give an order to all the soldiers, or to a set of selected personnel. Hence, routing protocols in such applications are required to provide secure communication with support for multicast routing.

Another area in which MANETs [2] can be deployed is collaborative and distributed computing. The requirement for a temporary communication network among a group of people in a conference, meeting or classroom necessitates the formation of a mobile ad hoc network. In such cases, the formation of a mobile ad hoc network with the necessary support for multicast routing can serve the purpose. Although these distributed file sharing applications may not require the level of security expected in a military environment, security aspects such as data integrity and data protection against unauthorized access are still needed. Emergency operations such as search and rescue can also earn great benefits from MANETs [3]. In situations where the infrastructure-based communication facilities are destroyed due to wars, terrorism or due to natural disasters such as hurricanes or earthquakes, immediate deployment of mobile ad hoc networks would be a good solution for coordinating rescue activities. The proposed solution will be incorporated on the above said three attacks in RSGM protocol and result are observed. Rest of this paper has organized as follows. Section 2 Implement the RSGM protocol in MANET. In Section 3 Prevention technique for attack in RSGM protocol. Section 4 Prevention technique for HMAC in RSGM protocol. Section 5 Simulation results. Finally, section 6 will be concluding the paper and also future work.

2. OVERVIEW OF RSGM PROTOCOL
RSGM supports a two-tier membership management and forwarding structure. At the lower tier, a zone structure is built based on position information and a leader is elected on demand when a zone has group members. A leader manages the group membership and collects the positions of the member nodes in its zone. At the upper tier, the leaders of the member zones report the zone membership to the sources directly along a virtual reverse-tree-based structure. If a leader is unaware of the position or addresses of the source, it could obtain the information from the Source Home. With the knowledge of the member zones, a source forwards data packets to the zones that have group members along the virtual tree rooted at the source. After the packets arrive at a member zone, the leader of the zone will further forward the packets to the local members in the zone along the virtual tree rooted at the leader.

- Group Membership Management
- Local Group Membership Management
- Membership Management at the Network Level

2.1 Group Membership Management

The group membership is managed at two tiers. RSGM is advantage of the virtual-zone based structure to efficiently track the group membership and member positions. In description, except when explicitly indicated, we use G, S and M, respectively, to represent a multicast group, a source of G and a member of G.

2.2 Local Group Membership Management

The group membership is first aggregated in the local zone and managed by the zone leader. When joining or leaving a group, a member M sends a message REFRESH (groupIDs, posM) immediately to its zone leader to notify its membership change, where posM is its position and groupIDs are the addresses of the groups in which M is a member. M also needs to unicast a REFRESH message to its zone leader every time interval Intval refresh to update its position and membership information. A member record will be removed by the leader if not refreshed within 2_ Intval refresh When M moves to a new zone, its next periodic REFRESH will be sent to the zone leader in the new zone. It will announce itself as the leader if the new zone does not have one. The moving node will still receive the multicast data packets from the old zone before its information is timed out at the leader of the old zone, which reduces the packet loss during the moving. For a leader node, if its distance to the zone border is shorter than a distance threshold and the zone is still a member zone, it will hand over its leadership by unicasting a LEADER message (carrying all the current group information) to the neighbor node in its zone which is closest to the zone center. The LEADER message will continue being forwarded toward the zone center until reaching a node which has no neighbor closer to the zone center than itself, and the node will take over the leadership and flood a LEADER within the zone.

2.3 Membership Management at a Network level

A zone leader needs to send REPORT every time interval Intvalzone to S to refresh its zone membership information. In case that S is the source of more than one multicast group, instead of sending a REPORT to S for each group, the leader sends one REPORT carrying all corresponding group IDs. S will remove a member-zone record if not refreshed within 2_Intrvalzone

2.4 Empty-zone handling

A zone may become empty when all the nodes move away. The probability that a zone is empty is approximately $P = e^{-pr2}$ when the node density is _ and the zone size is r. Let's calculate the probability of zone being empty for two typical node densities and zone sizes:

- When _ = 60 nodes/km2, r = 100 m, P = 0:55
- When _ = 20 nodes/km2, r = 400 m, P = 0:04.

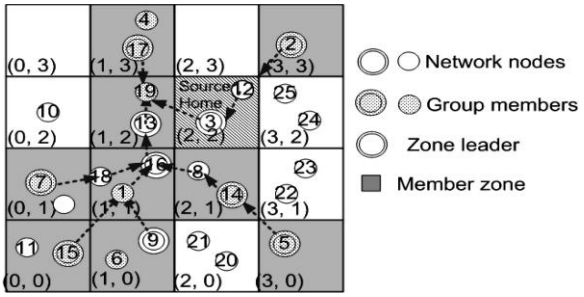

Fig 1: The aggregation of REPORT messages and the virtual-reverse tree formulation.

We can see that in either case, the probability of a zone being empty is not negligible. Therefore, it is critical to address the empty-zone problem. When a member zone of G is becoming empty, the moving out zone leader will notify S immediately to stop sending packets to the empty zone. If the moving out leader fails to notify S (e.g., the leader suddenly dies), the packet forwarded the empty zone will finally be dropped without being delivered. The node which drops the packet will notify S to delete the zone from its zone list. A false deletion will be corrected when S receives the periodic membership reporting again from the corresponding zone.

2.5 Message aggregation

As compared to local messages, control messages sent at the network tier would generally traverse a longer path. To minimize control overhead, we consider a virtual reverse-tree-based aggregation scheme (Figure 1), with which all the control messages sent toward the same destination (e.g., the source S) will be aggregated to further reduce control overhead. Different from other tree based multicast protocols, no explicit tree structure needs to be maintained, which avoids the overhead and improves the robustness. Specifically, the periodic REPORT messages can be aggregated and forwarded along the reverse tree. To facilitate the message aggregation, S schedules the periodic REPORT sending for the member zones. S inserts the next periodic reporting time t into the data packets sent out. The leader of a member zone schedules its next periodic REPORT to S at time $t+\Delta t$, where Δt t is inversely proportional to its distance to S. The zone leaders will form an upstream and downstream relationship according to their distances to S. Generally, the leaders farther away from S have a shorter Δt and will send the REPORTs earlier than the upstream zone leaders, while strict timing is not needed. When a REPORT message reaches a member zone, it is forwarded to the leader first. When an upstream zone leader receives REPORTs from downstream zone leaders, if it has not sent out its REPORT, it will aggregate these REPORTs with its own REPORT, and send out the REPORT at its scheduled time. As a result, the structure as shown in Fig 1 The REFRESH messages sent by member nodes to the zone leader can be similarly aggregated and sent through the virtual reverse tree.

2.6 Multicast Packet Delivery

A source needs to send the multicast packets reliably to the group members. With the membership management, the member zones are recorded by source S, while the local group members and their positions are recorded by the zone leaders. Multicast packets will be sent along a virtual distribution tree from the source to the member zones, and then along a virtual distribution tree from the zone leader to the group members.

The multicast packets are first by S to member zones toward their zone centers. S sends a multicast packet to all the member zones, and to the member nodes in its own zone through the zone leader. For each destination, it decides the next hop by using the geographic forwarding strategy. After all the next hops are decided, S unicasts to each next-hop node a copy of the packet which carries the list of destinations that must be reached through this hop. An intermediate node makes its forwarding decisions based on the destination position inserted in the packet header by the source and the positions of its one-hop neighbors learned from the periodic beaconing of the neighbors. A multicast source broadcasts Join-Query messages to the entire network periodically. An intermediate node stores the source ID and the sequence number, and updates its routing table with the node ID (i.e., backward learning) from which the message was received for the reverse path back to the source. A receiver creates and broadcasts a Join Reply to its neighbors, with the next-hop node ID field filled by extracting information from its routing table. The neighboring node whose ID matches that in the message broadcasts its own Join Table built upon matched entries. This whole process constructs (or updates) the routes from sources to receivers and builds a mesh of nodes, the forwarding group. Due to the protocols design issues like scalability, robustness, and efficiency under the dynamic environment. So we have been implemented by prevention techniques for each and every possible type of attacks in the RSGM protocol. These are attacks as Flooding, blackhole and Wormhole attacks.

3. SECURITY THREATS IN MANETs

The current Mobile ad hoc networks allow for many different types of attacks. Although the analogous exploits also exist in wired networks but it is easy to fix by infrastructure in such a network. MANETs [12] are basically vulnerable to two different types of attacks: active attacks and passive attacks. Active attack is an attack when misbehaving node has to bear some energy costs in order to perform the threat. On the other hand, passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered as malicious while nodes that make passive attacks with the aim of saving battery life for their own communications are considered to be selfish. This paper focuses on the vulnerabilities and exposures in the mobile ad hoc network.

3.1 Attacks against RSGM

3.1.1 Black hole Attack

In a blackhole attack [4] [5], is one such attack in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. This attack Fig 2 aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacks.

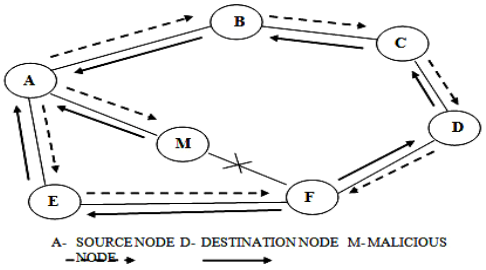

Fig: 2 Blackhole Attack

3.1.2 Wormhole attack

In a wormhole attack [7] [8], an attacker receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunneled. This tunnel between two colluding attacks is known as a wormhole.

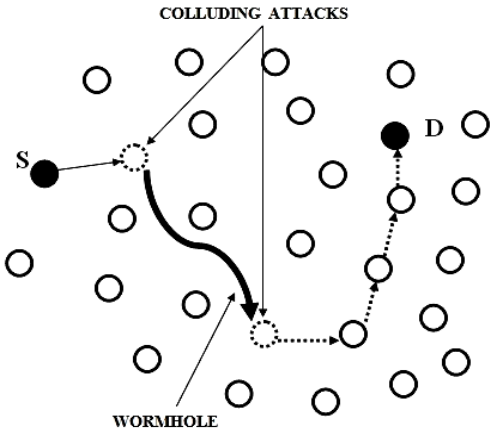

Fig: 3 Wormhole Attack

3.1.3 Flooding attack

The aim of the flooding attack [10] [11], is to exhaust the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. A malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network.

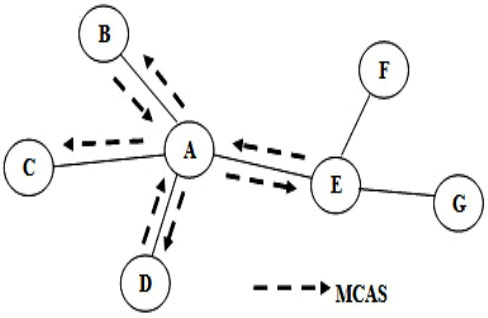

Fig: 4 Flooding Attack

4. SOLUTION FOR PREVENTING BLACK HOLE, WORMHOLE AND FLOODING

This solution aims at preventing the attacks by establishing a secure between the nodes. The usage of message authentication codes for the process of identification of confidence and authentication nodes among MANET nodes. The motivation for the use of HMAC [16] is that, it gives confidence and authentication to the source node or the owner about the security participating nodes in the network. Here a hash function is transmitted or shared among the multiple individuals in the network that are under the process of encryption and decryption. The objective is to maintain the security of the nodes that are present in the network. Maintaining the integrity of the data during transmission to the other nodes adds difficulties to the security services provided to the MANETs [13]. To overcome this problem we use of encryption algorithm .In providing a way to check the integrity of information transmitted over or stored in an unreliable medium is a prime necessity in the world of open computing and communications. Mechanisms that provide such integrity checks based on a secret key are usually called message authentication codes (MACs). Typically, message authentication codes are used between two parties that share a secret key in order to authenticate information transmitted between these parties. This Standard defines a MAC [17] that uses a cryptographic hash function in conjunction with a secret key. This mechanism is called HMAC [HMAC]. HMAC [18] shall use an Approved cryptographic hash function FIPS. HMAC uses the secret key for the calculation and verification of the MACs.
The main goals behind the HMAC construction are:

- To use available hash functions without modifications; in particular, hash functions that perform well in software, and for which code is freely and widely available.
- To preserve the original performance of the hash function without incurring a significant degradation,
- To use and handle keys in a simple way.
- To have a well-understood cryptographic analysis of the strength of the authentication mechanism based on reasonable assumptions on the underlying hash function.
- To allow for easy replaceability of the underlying hash function in the event that faster or more secure hash functions are later available.

The purpose of a MAC is to authenticate both the source of a message and its integrity without the use of any additional mechanisms. HMACs [18] have two functionally distinct parameters, a message input and a secret key known only to the message originator and intended receiver(s). Additional applications of keyed-hash functions include their use in challenge-response identification protocols for computing responses, which are a function of both a secret key and a challenge message. An HMAC [18] function is used by the message sender to produce a value (the MAC) that is formed by condensing the secret key and the message input. The MAC [17] is typically sent to the message receiver along with the message. The receiver computes the MAC on the received message using the same key and HMAC function as was used by the sender, and compares the result computed with the received MAC. If the two values match, the message has been correctly received and the receiver is assured that the sender is a member of the community of users that share the key.

4.1 HMAC Parameter and Symbol

HMAC uses the following parameters:

B	- Block size (in bytes) of the input to the Approved hash function.
H	- An Approved hash function.
ipad	- Inner pad; the byte x'36' repeated *B* times
K	-Secret key shared between the originator and the intended receiver(s).
*K*0	-The key *K* after any necessary pre-processing to form a B bytes key .
L	-Block size (in bytes) of the output of the Approved hash function.
Opad	- Outer pad; the byte x'5c' repeated *B.* times.
t	- The number of bytes of MAC.
text	-The data on which the HMAC is calculated text does not include paddy key. The length of text is n bits, where 0 £ $n < 2B - 8B$.
x'*N*	-Hexadecimal notation, where each Symbol in the String 'N' represents 4 binary bits.
‖	-Concatenation
⊕	- Exclusion or operation

4.2 Algorithm to prevent the attacks

To compute a MAC over the data '*text*' using the HMAC function, the following operation is performed:

MAC (text)t = HMAC(K, text)t = H((K0 ⊕ opad) || H((K0 ⊕ ipad) || text))t

- Step 1
- If the length of $K = B$: set $K0 = K$. Go to step 4.
- Step 2
- If the length of $K > B$: hash *K* to obtain an *L* byte string, then append (*B*-*L*)
- zeros to create a B-byte string *K*0 (i.e., *K*0 = H(*K*) ‖ 00...00). Go to step 4.
- Step 3
- If the length of $K < B$: append zeros to the end of *K* to create a *B*-byte string *K*0
- (e.g., if *K* is 20 bytes in length and $B = 64$, then *K* will be appended with 44
- zero bytes 0x00).
- Step 4
- Exclusive-Or *K*0 with *ipad* to produce a *B*-byte string: ***K*0 ⊕ *ipad***.
- Step 5
- Append the stream of data '*text*' to the string resulting from step 4:
- **(*K*0⊕ *ipad*) ‖ *text*.**
- Step 6
- Apply *H* to the stream generated in step 5: **H((*K*0 ⊕ *ipad*) ‖ *text*).**
- Step 7
- Exclusive-Or *K0* with *opad*: ***K*0 ⊕ *opad*.**
- Step 8
- Append the result from step 6 to step 7:
- **(*K*0 ⊕ *opad*) ‖ H((*K*0 ⊕ *ipad*) ‖ *text*).**
- Step 9
- Apply *H* to the result from step 8:
- ***H*((*K*0⊕ *opad*)‖ *H*((*K*0 ⊕ *ipad*) ‖ *text*)).**
- Step 10
- Select the leftmost *t* bytes of the result of step 9 as the MAC.

The HMAC [17] algorithm is specified for an arbitrary Approved cryptographic hash function, *H*. With minor modifications, an HMAC implementation can easily replace one hash function, *H*, with another hash function, *H'*. Conceptually, the intermediate results of the compression function on the *B*-byte blocks ($K0 \oplus ipad$) and ($K0 \oplus opad$) can be precomputed once, at the time of generation of the key *K*, or before its first use. These intermediate results can be stored and then used to initialize *H* each time that a message needs to be authenticated using the same key. For each authenticated message using the key *K*, this method saves the application of the hash function of *H* on two *B*-byte blocks (i.e., on ($K \oplus ipad$) and ($K \oplus opad$)). This saving may be significant when authenticating short streams of data. These stored intermediate values shall be treated and protected in the same manner as secret keys. Finally the encrypt and decrypt will be same original message in the security. The HMAC algorithm is used to prevent blackhole, wormhole and flooding attack and the protocol is secured.

5. SIMULATION RESULTS

Table 1. Simulation Parameter

Parameters	Values assigned
RSGM refreshment interva	0.33 seconds
Channel capacity	2 Mbps
Packet size	128 bytes
Traffic model	Multicast constant bit rate
Mobility model	Random way-point
Queuing policy	First-in-first-out

We conducted our experiments using NS2 Simulation 2.28.Our simulated network consists of 50 mobile nodes placed randomly within a 1000 m x 1000 m area. Each node has a transmission range of 250 m and moves at a speed of 1 m/s. The total sending rate of all the senders of the multicast group, i.e., the traffic load, is 1 packet/s. We use a low traffic load value to highlight the effects of the attacks on packet loss rate, as opposed to packet loss due to congestion and collisions resulting from a high traffic load. The mobility model chosen for a mobile node was the *random way-point* model. A mobile node begins by staying in one location for a pause time of 30 seconds. Once this time expires, the mobile node chooses a random destination in the simulation area and then travels toward the newly chosen destination. Upon arrival, the mobile pauses for 0.33 seconds before starting the process again.

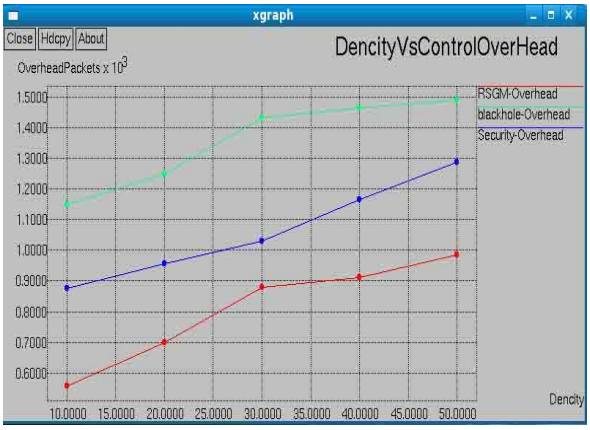

Fig 5: Blackhole Attack – Control Overhead

Control Overhead decreases on an average by **4%** when secure key exchange solution is provided to prevent the black hole attack in RSGM.

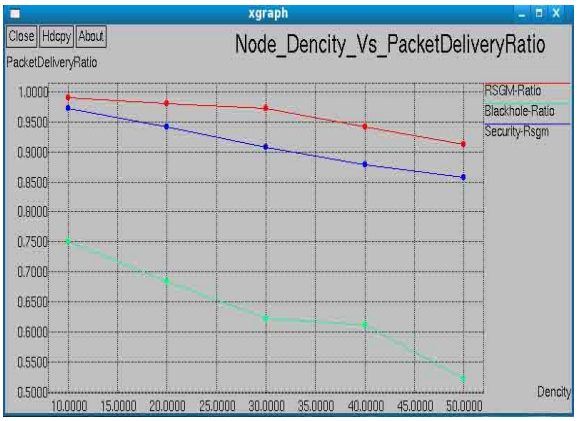

Fig 6: Blackhole Attack – Packet Delivery Ratio

Packet delivery ratio increases on an average by **20%** when secure key exchange solution is provided to prevent the black hole attack in RSGM.

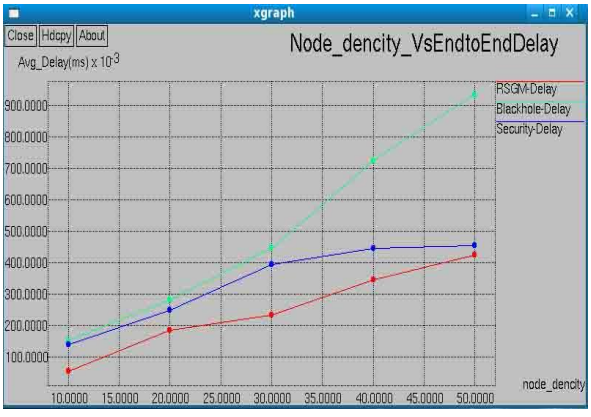

Fig 7: Blackhole Attack – End to End Delay

End to End Delay decreases on an average by **3.5%** when secure key exchange solution is provided to prevent the black hole attack in RSGM.

Fig 8: Wormhole Attack – Control Overhead

Control Overhead decreases on an average by **3.8%** when secure key exchange solution is provided to prevent the Worm hole attack in RSGM.

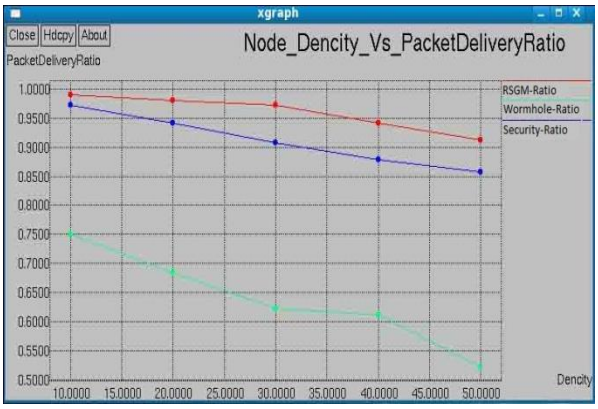

Fig 9: Wormhole Attack –Packet Delivery Ratio

Packet delivery ratio increases on an average by **17%** when secure key exchange solution is provided to prevent the worm hole attack in RSGM.

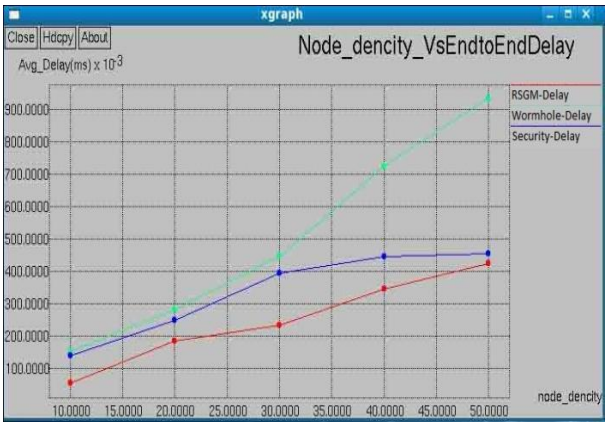

Fig 10: Wormhole Attack – End to End Delay

End to End Delay decreases on an average by **3%** when secure key exchange solution is provided to prevent the worm hole attack in RSGM

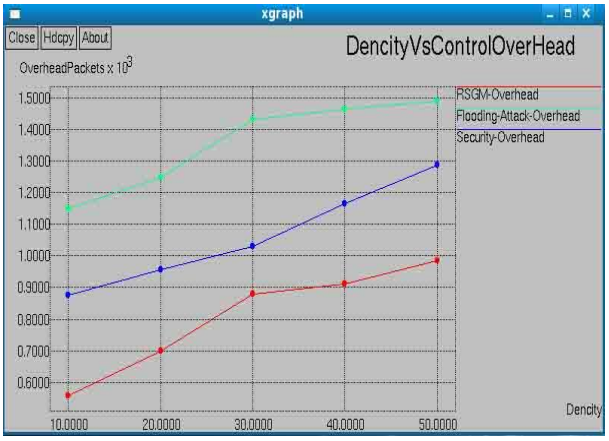

Fig 11: Flooding Attack – Control Overhead

Control Overhead decreases on an average by **5%** when secure key exchange solution is provided to prevent the flooding attack in RSGM.

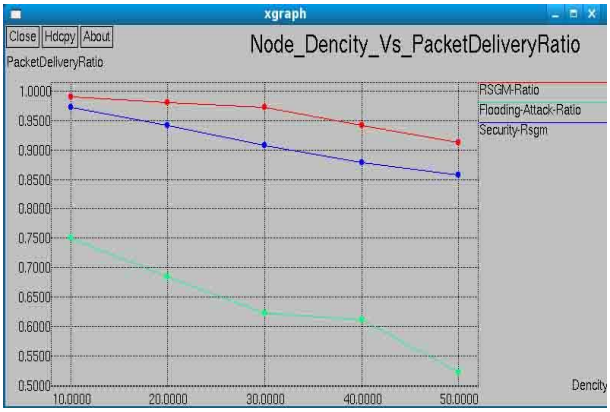

Fig 12: Flooding Attack – Packet Delivery Ratio

Packet delivery ratio increases on an average by **25%** when secure key exchange solution is provided to prevent the flooding attack in RSGM.

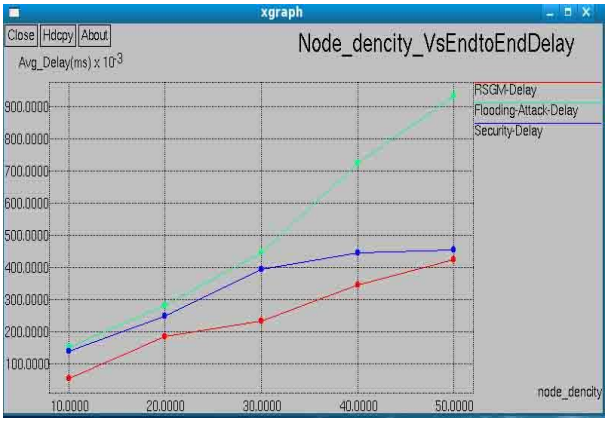

Fig 13: Flooding attack – End to End Delay

End to End Delay decreases on an average by **5%** when secure key exchange solution is provided to prevent the flooding attack in RSGM.

6. CONCLUSION AND FUTURE WORK

A tree based protocol namely RSGM is taken and a complete analysis is done sorting out the vulnerability spots in the protocol. The protocol is analyzed for various kinds of attacks such as flooding, blackhole and wormhole. A comprehensive survey has been done on various types of attacks like blackhole attack, flooding, and wormhole and all the possible solutions are listed. The scenarios for these attacks are identified and are generated and a unique solution has been proposed for overcoming these attacks. Thus the solution that has been proposed for the security of MANETs against attacks like flooding, wormhole, blackhole etc, has been achieved. This provide a secure routing for all tree based multicast routing protocols such as RSGM, EGMP etc., With this scheme it is easier for the source node to identify the nodes that enter the network without authorization. This solution is very much applicable in the situation where the attacker enters the network and tries to impersonate themselves as legitimate nodes in the network. This solution is designed only for the external attacker that claims to be as genuine nodes. The future enhancement for this scheme is to provide suitable solution for other type of attackers and also to extend the solution for the mesh based protocols also.

7. REFERENCES

[1] K. Aishwarya, N.Kannaiah Raju and A. Senthamarai SelvanCounter "Measures Against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol In Mobile ADHOC Networks" -*International Journal of Technology And Engineering System*(IJTES) Jan – March 2011

[2] Semih Dokurer, Y.M. Erten and Can Erkin Acar "Performance analysis of ad-hoc networks under black hole attacks" IEEE 2007.

[3] Asmaa Adnane and Christophe Bidan, Rafael Timoteo de Sousa Junior " Trust-based countermeasures for securing OLSR protocol", *International Conference on Computational Science and Engineering.*

[4] E.A.Mary Anita, V.Vasudevan, "Black Hole Attack on Multicast Routing Protocols", *jcit. Vol.4.issue2.anita.*

[5] Mohammad Al-Shurman , Seong-Moo Yoo and Seungjin Park **"**Black Hole Attack inMobile Ad Hoc Networks" *ACM* April-2004.

[6] Hesiri Weerasinghe, Huirong Fu "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Network: Simulation Implementation and Evaluation".

[7] Weicho Wang, Bharat Bhargava, Yi Lu, Xiaoxin Wu "Defending against Wormhole Attacks in Mobile Ad Hoc Networks", Wiley Journal Wireless Communication and Mobile Computing(WCMC).

[8] S.Vijayalakshmi and S.Albert Rabara "Weeding Wormhole Attack in MANET Multicast Routing using Two Novel Techniques – LP3 and NAWA2" *International Journal of Computer Applications* (0975 – 8887) vol. *16– No.7,* February 2011.

[9] Preeti Nagrath, Bhawna Gupta " Wormhole Attacks in Wireless Adhoc Network and their Counter Measure: A Survey" IEEE 2011.

[10] Nam Uk Kim, HyunSu Lim, HongShik Park and Minho Kang "Detection of Multicast Video Flooding Attack Using the Pattern of Bandwidth Provisioning Efficiency", IEEE vo*l. 14 No. 12*, December 2010.

[11] Hyojin Kim, Ramachandra Bhargav Chitti, and JooSeok Song "Novel Defense Mechanism against Data Flooding Attacks in Wireless Ad Hoc Networks", IEEE Transaction on Consumer Electronics, v*ol. 56, No 2*, May 2010.

[12] W. Wu, J. Cao, J. Yang, and M. Raynal, "Design and Performance Evaluation of Efficient Consensus Protocols for Mobile Ad Hoc Networks," IEEE Trans. Computers, *vol. 56, no.8, pp. 1055-1070*, Aug. 2007.

[13] J. Li, J. Jannotti, D.S.J.D. Couto, D.R. Karger, and R. Morris, "A Scalable Location Service for Geographic Ad Hoc Routing," Proc. MOBICOM, pp. 120-130, 2000. 11] J.J. Garcia-Luna Aceves and E.

[14] M. Gerla, S.J. Lee, and W. Su, "On-Demand Multicast Routing Protocol (ODMRP) for Ad Hoc Networks," Internet Draft, draf tietf- manet-odmrp-02.txt, 2000.