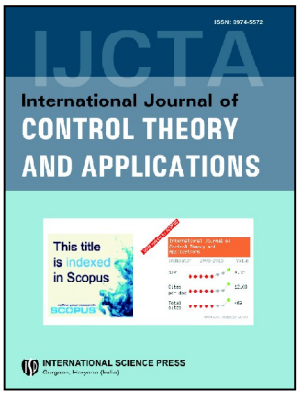

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 9 • Number 49 • 2016

A Secure and Reliable Cooperative Multicast Routing Based on Hop Tree in Ad-Hoc Networking

Perala Srikanth, Joshua Reginald Pullagura and Yaminilakshmi Valiveti

Dept. of Electronics and Communication Engineering, VFSTR University, India-522213, E-mail: srikanth.perala@gmail.com

Abstract: The MANET is a new emerging communication network which consists of several devices called as nodes or motes. As the name specifies that nodes are having mobility nature and these are operated with the help of energy source only. Due to the frequent changes in the position of nodes the battery squanders quickly. The data packets in the MANETs are moved accordingly with some routing protocols. During routing it is more prone to attack the network and sometimes causes security issue. The major security pitfall is vampire attack. This work is mainly on diminishing the vampire attacks which drains the energy from the nodes which leads to network failure in traditional protocols like AODV, DSR and DSDV. To overcome these attacks, we proposed some modifications to the existing algorithm CMAODV (Cooperative Multicast Ad-hoc Ondemand Distance Vector). The utmost ease with this protocol is it consists of static nodes, so that vampire attack poses a serious attack on AODV which makes energy ingestion between the nodes. These vampire attacks are protocol independent instead they attack the properties like link state, distance vector and beacon routing. Predominantly there are two types of vampire attacks are existed, namely carousel and stretch. Whenever these attacks are occurred then energy consumption is more compared with the normal case and the packets reach its destination latterly. The CMAODV is less prone to vampire attack and also reduces the energy consumption, delay while routing and provides more throughput when compared to AODV, DSR.

Keywords: MANETS, DSR, AODV, CMAODV, Vampire

1. INTRODUCTION

The communication is much important in these days. Wireless communication is one of the current emerging areas of research. It became so popular in last few years and became an integral part of the human life. Apart from the conventional wireless communications techniques like cellular phones Wi-Fi and Blue tooth, there are emerging techniques for wireless communication coming into picture which include Mobile Adhoc Networks and Wireless sensor networks. As the technology emerges the requirements of the users also increased. To meet those the MANETs are introduced. MANETs are self-configuring networks and doesn't require any central monitoring like base station, control system etc. Adhoc allows the nodes within range of each other to discover easily and to communicate without the involvement of central administration. The nodes which are involved in exchanging of data are determined dynamically. The Wireless sensors are placed strategically inside a physical medium so that they can measure various physical, biological and environmental parameters from the surrounding

selected area and gives this information to the system. The network topology keeps changing constantly because of the mobility of the nodes and hence they are prone to fail. Even though there are having the mobility nature these are easy to reconfigure. The major aspect with MANETs is it plays a prominent role in military wide and navy area where there is no chance to establish infrastructured network. MANETs are also self-alleviate. These sensor nodes or devices will have limited power, limited memory and low computational capabilities. As these nodes are all operated with the help of energy source the usage is more important. In the most of the cases the resource depletion attack enters into the network and make power dropping of the network. In many of the applications the recharging or the replacement of battery is improbable. The vampire attack is of such type, if it is detected then the energy of node as well as the network life time increases.

2. ROUTING IN MANETS

Routing is the process of governing the format to the data packets to reach its destination. The Adhoc networks allows routing protocols to discover the routes instead of following the fixed topology. The routing protocol must consider some metrics like bandwidth, energy, computational capacity, memory. The routing follows two activities, 1. It first discovers the paths from source to destination 2. Sends the data along the optimal path. The classification of routing includes static, dynamic routing. The static routing refers to routing that maintains routing tables and follows the predefined paths. The information is included manually into the tables. The major limitation with static routing is, if the nodes are added/removed from the network then it is the administrator role to update the statistics but it is not possible all the time. The static routing is independent on the state of the nodes i.e, whether they are active, idle, sleep. While in dynamic routing, the routes are determined dynamically with the use of hello/beacon packets. The information is updated automatically and there is no need of administrator. The state of nodes shows impact on routing approach.

3. TRADITIONAL ROUTING PROTOCOLS

DSDV: Destination sequenced distance vector routing and it is of proactive type. The protocol maintains the routing table with the information like source, destination address and hop count. To maintain the consistency in the routing table the updates must be transmitted periodically. Even when the routes are not necessary the periodic updates are transferred. Due to this battery usage is increased and also more bandwidth is consumed. This protocol only suits for less number of nodes. DSDV doesn't supports for high dynamic networks.

AODV: It is an Adhoc On demand Distance Vector Routing. It is an on demand routing protocol. This protocol responds fastly to the link changes and link failures and also provides loop free routing. It eliminates the need of periodic beaconing and creates new routes on demand. The routing protocol follows two process 1. Route discovery 2. Route maintenance.

Route discovery: The route discovery phase includes route request (RREQ) and route reply (RREP) messages. When a route to the specified node is needed, the source node broadcast RREQ in the network and finds the optimal path. The RREQ contains the broadcast ID, destination address and sequence number, source address and destination number.

Whenever a node receives RREQ/RREP its sequence number is increased. The information is stored in the nodes routing table. The destination node sends the RREP to the source by including the destination address and sequence number, lifetime, source address. The RREP travels along the reverse path to establish forward links.

Route maintenance: The route is maintained by HELLO and RERR packets. Whether the node is in active position or not is determined by the use of HELLO messages. If the node receives the message in time then it is referred as active node otherwise the RERR message is sent to the source node. Then it reinitiates the other route by removing the dropped nodes.

DSR: DSR refers to Dynamic Source Routing and it is also an on demand routing. It is also called source routing. The route discovery process is based on flooding. The source sends the RREQ throughout the network like flooding. If the RREQ reaches the destination then it sends reply with RREP packet along the reverse route. For a single RREQ there exists several RREP. The routes are all stored in its cache. The whole route is carried as a message overhead. To avoid the RREQ travel forever in the network just discard further RREQ with the same identifier.

4. RELATED WORK

Due to the characteristics like open access and deployment, infrastructureless, wireless communication the MANETs are easily overwhelm with the malicious nodes. The malicious node which enters into the network causes different problems like denial of service, energy draining, flooding, eavesdropping etc. The attacks are mainly classified into active and passive attacks.

Passive attack

These type of attacks doesn't cause any harm to the network. It simply monitors and captures the entire information regarding nodes and data. Passive attack don't inject any other data into the network. This collects the information and made available that to active attack.

The examples of passive attacks are eavesdropping, snooping.

Active attack

The active attacks are harmful to the network. These lead to change in the network traffic, injects the wrong information and modifies the confidential information. The examples are black hole, wormhole, vampire attack etc.

VAMPIRE ATTACK

The vampire attack is one of the energy draining attack. Vampire attack means creating and sending messages by malicious node which causes more energy consumption by the network leading to slow depletion of node's battery life. It again classified into carousel and stretch.

(A) Carousel attack

In this attack the rival node sends the data packet with composed routes. The provided route is with series of loops means the same node is repeated so many times. Due to this loop routes the length of the path increases. The theoretical limit provided for this attack is $O(\lambda)$, where λ is maximum length of the route. For every message there occurs an increase in energy up to the factor of 3.96. The energy consumed by carousel attack is 4 times of the energy consumed in normal case.

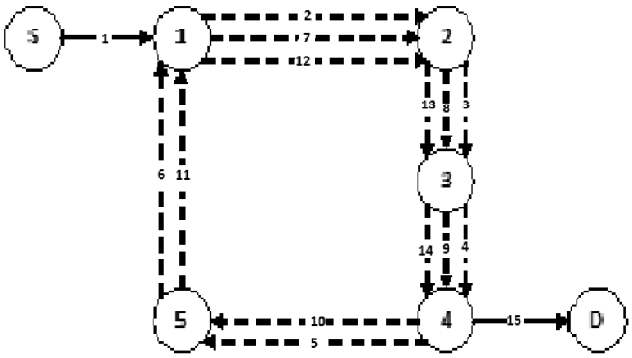

Figure 1: Carousel attack

In carousel attack, the entering of the malicious node makes the path by looping. In the above figure the carousel attack is shown. Instead of going from source to destination in a path, it creates looping structure and revisit the same path so many times and then reaches the destination. In this network only one vampire is present. Here the node 4 is a vampire node and it creates looping structures. The actual path is S-1-2-3-4-D but it creates loop from the node 5 and traverse through the path 5-1-2-3-4 several times and then reach its destination node. By this the battery of the node degrades and also delay is introduced by increasing the time consumption to reach the end node.

(B) Stretch attack

The stretch attack causes potential problems and pilfer the resources. The malicious node creates the longer paths in the network. The data packet traverses through more number of nodes than the optimal number of nodes. The stretch attack is given with the theoretical limit as O(N, λ), where N is total number of nodes in the network and ë is maximum allowable path length. The stretch attack causes increase in data packet length since it is undergone processed by more number of nodes.

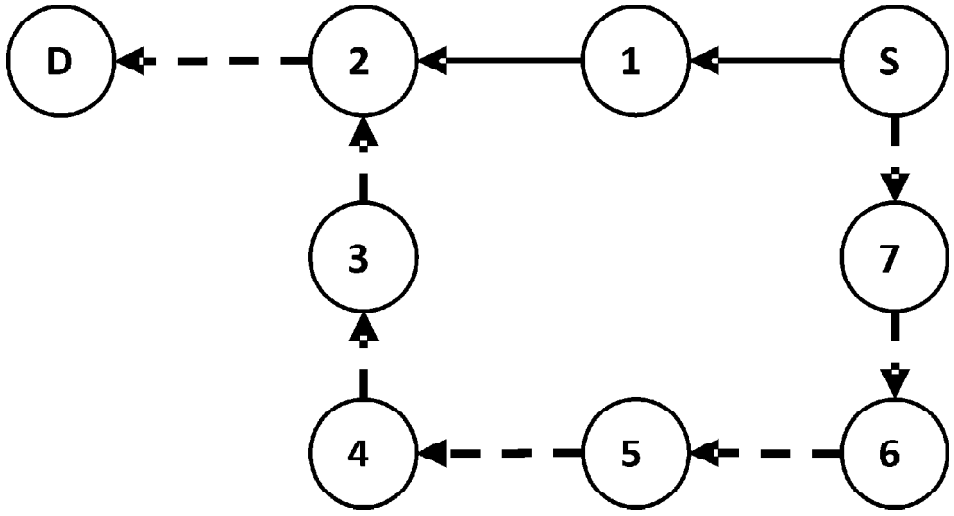

Figure 2: Stretch attack

In stretch attack, instead of sending the data through optimal path it selects the longest route to reach the destination node. In this network the node 1 has shortest path to destination but it doesn't allows the source to reach since the vampire is attacked on that node. The path to be followed to reach its destination is S-1-2-D but the path taken by the protocol is S-7-6-5-4-3-2-D. In this way the stretch attack leads to wastage of energy of more number of nodes. The energy consumption is in order of magnitude, which depends on the position of attacker node.

5. PROPOSED WORK

The major challenge in Adhoc sensor networks is the energy, since all nodes are operated with the usage of battery only. The nodes will vary their positions with time, while in this time it is possible for the vampire node to get introduced into the network. The vampire makes the energy to drain fastly. Because it creates looping in the routes or creates the longest path. To overcome this vampire attack a new protocol called CMAODV is introduced. The CMAODV maintains the routing table and records the entry of every node. The nodes in the network are provided with some initial sequence number. During routing in CMAODV, the source node first sends the RREQ among its neighbors. It may be reached to destination or intermediate node. After the node

receiving the request it reverts back the RREP to the source node. The source node is called as head node. The nodes surrounding the head node are known as cooperative nodes. The head node starts route search and identifies the super node with the help of cooperative nodes. The super node is elected based on the highest sequence number. The sequence number depends on the number of RREQ received, RREP sent. There are two occurrences for increasing the sequence number of the node: 1.whenever the RREQ is received from the source 2. When it sends the RREP in response. After the identification of super node,the head node sends the data to super node. Now the super node itself acts as head node and repeats with the above process until it reaches the destination. Each route is provided with timeout packets. After timeout this route is not available for routing.

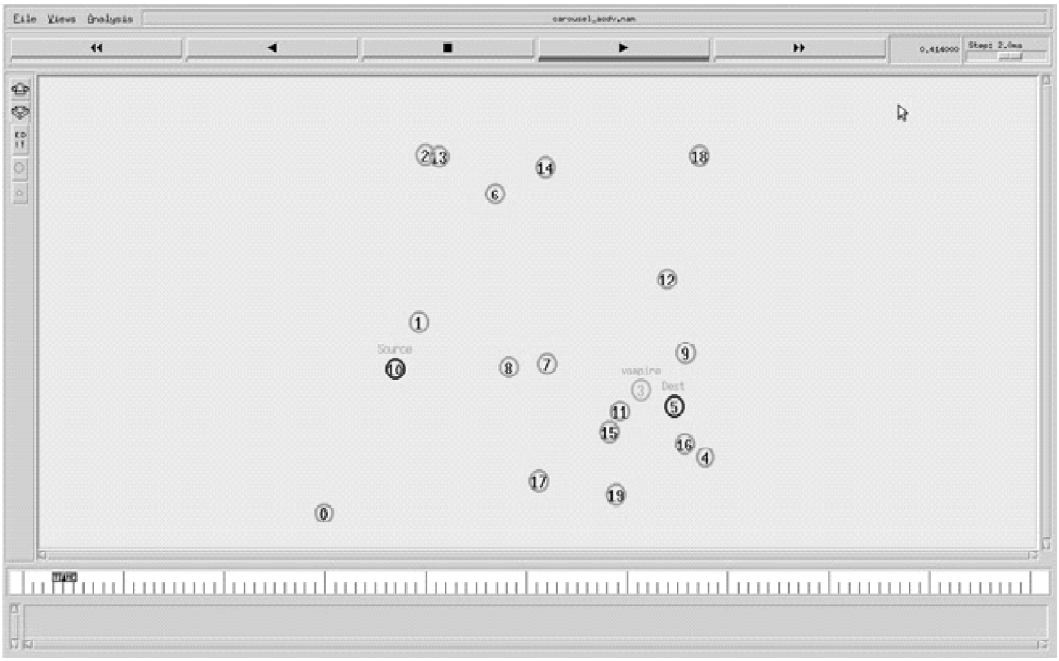

Figure 3: CMAODV Routing

In this scenario the source node is marked as 10 and destination is 5. During the routing setup phase the source flooded the route request, the nodes1,8,7 surrounding the source receives it. Again the node 8 receive the RREQ from the node 1 and its sequence number increases and become as super node. Now the data is transmitted via the super node. It again starts search for the destination and broadcasts the route request. During this the vampire node 3 accepts the RREQ and sends back the RREP. Even though the malicious node is injected into the network it doesn't show the impact since each node is allowed to identify the super node or destination node. During this if vampire tries to make other node as super node also it fails, because the super node is depending on the sequence number only. So in this way CMAODV overcomes the vampire attack.

The flowchart shown here explains the working involved in CMAODV.

1. At first the route search is starting from the head node.
2. It floods the RREQ to its neighbors called as cooperative nodes. The node gets activated and sends the RREP if accepts the request.
3. The sequence number of a node increases with the RREQ from the source/ with RREP from the destination.
4. Now consider the node with highest sequence number among all the neighboring nodes and mark it as super node. The nodes with lowest sequence number would remain as cooperative nodes.

5. Later on data packets will transfer from head to super node.
6. If the destination is detected by super node then data is transmitted to it. Otherwise it continues with route search to the destination node.

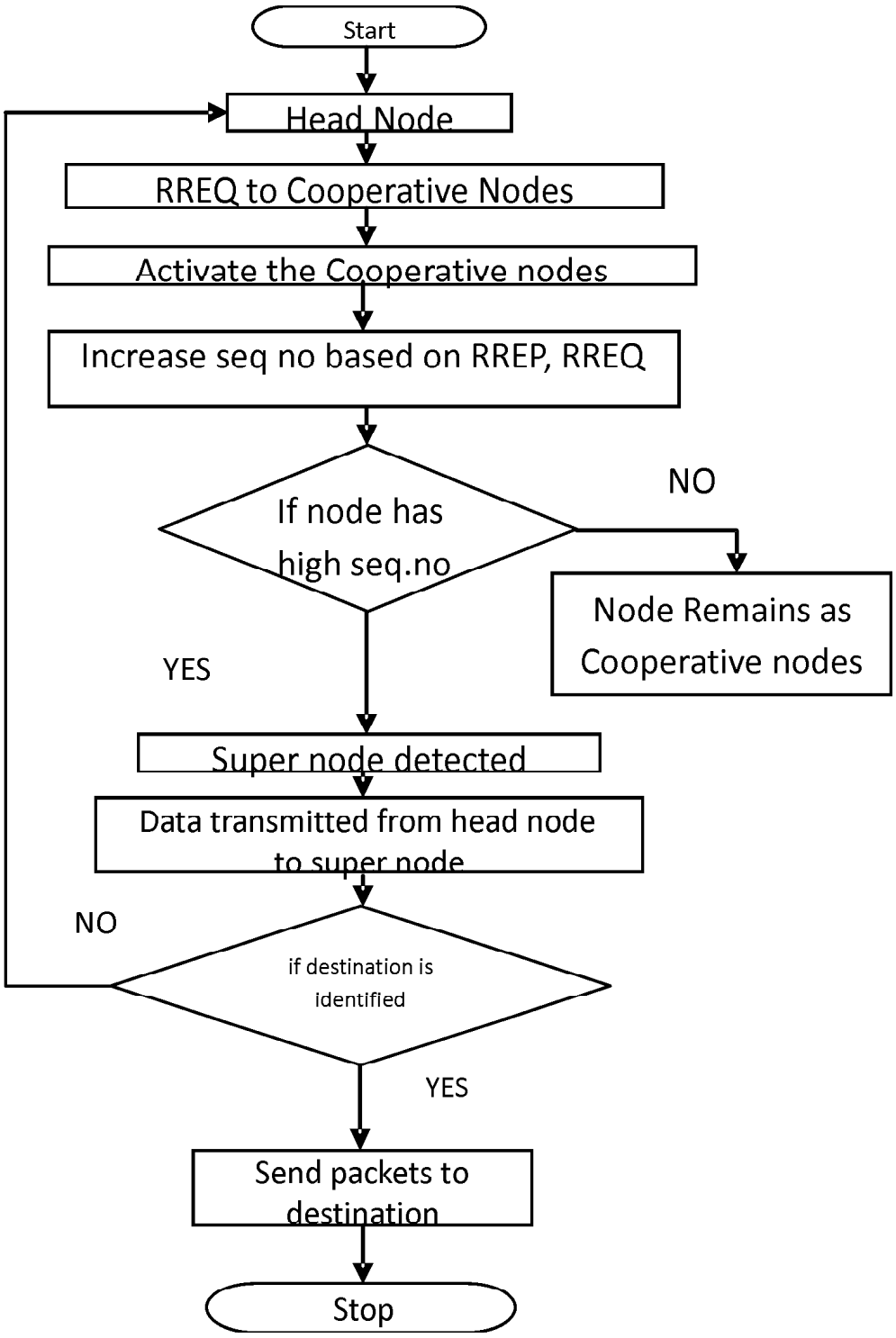

Figure 4: CMAODV Flow chart

6. SIMULATION SCENARIO

The simulation is carried out using 20 nodes in network simulator 2. The carousel attack and stretch attack on DSDV, AODV, DSR are shown below. Along with these the remaining energy in CMAODV is compared with the energy remained in case of carousel and stretch attack on these traditional protocols. The simulation parameters are

Simulation tool	Ns-2.35
Number of nodes	20,30,40
Routing protocols	DSDV, AODV, DSR, CMAODV
Traffic source	TCP
Simulation Duration	50s
Initial energy	100J
Transmission power	0.25nW
Receiving power	0.25nW
Mobility Model	Random way point
Traffic type	CBR
MAC	802.11
Simulation area	750*650
Antenna Type	Omni Antenna

From the Fig 4-6 the remaining energies in case of normal AODV/DSDV/DSR and the AODV/DSDV/DSR with carousel attack are compared.

In Fig. 7 the remaining energies of AODV/DSDV/DSR under carousel attack and CMAODV are compared.

In Fig. 8 the remaining energies of normal AODV,DSDV,DSR are plotted.

The remaining energies in case of normal AODV/DSDV/DSR and the AODV/DSDV/DSR under stretch attack are shown in Fig. 9-Fig. 11.

In Fig. 11 the remaining energies of AODV/DSDV/DSR under stretch attack and CMAODV is plotted.

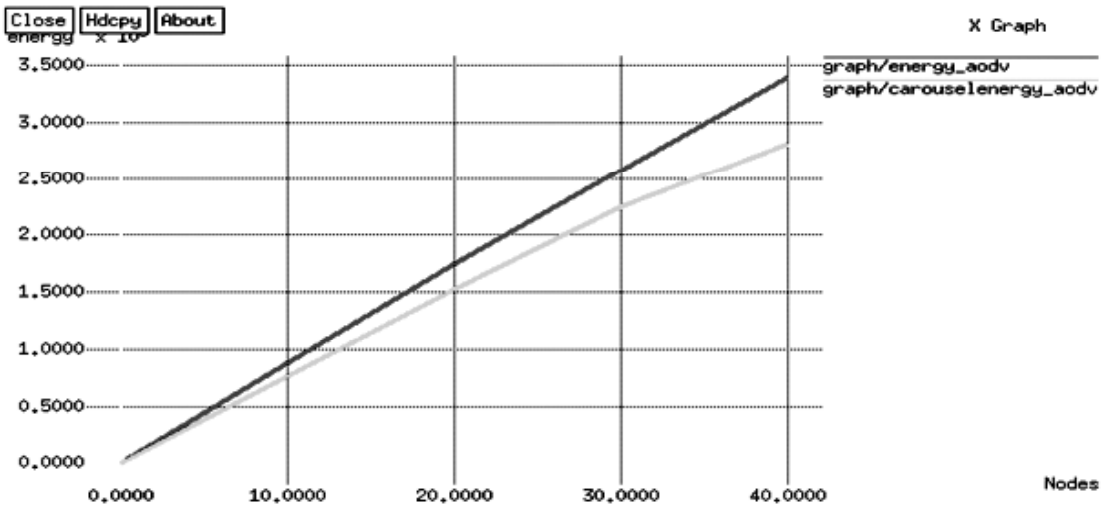

Figure 4: Comparison of remaining energies of AODV and carousel attack on AODV

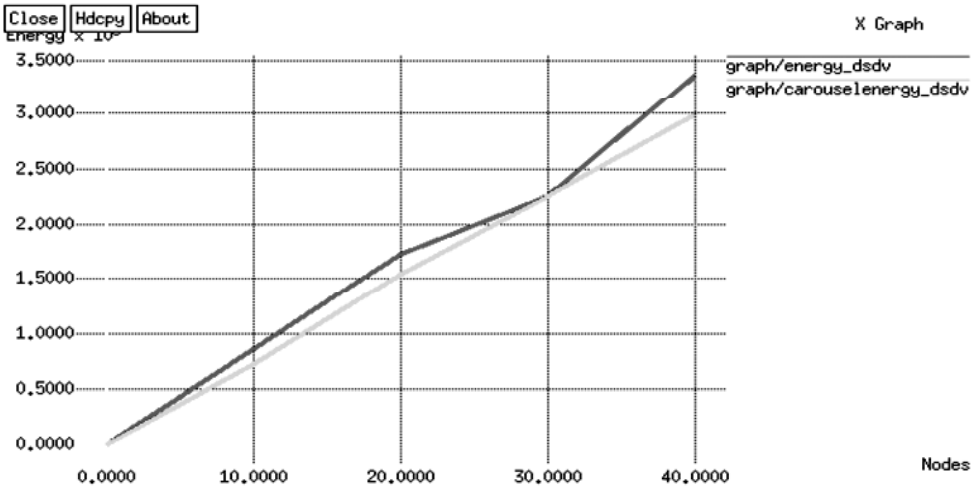

Figure 5: Comparison of remaining energies of DSDV and carousel attack on DSDV

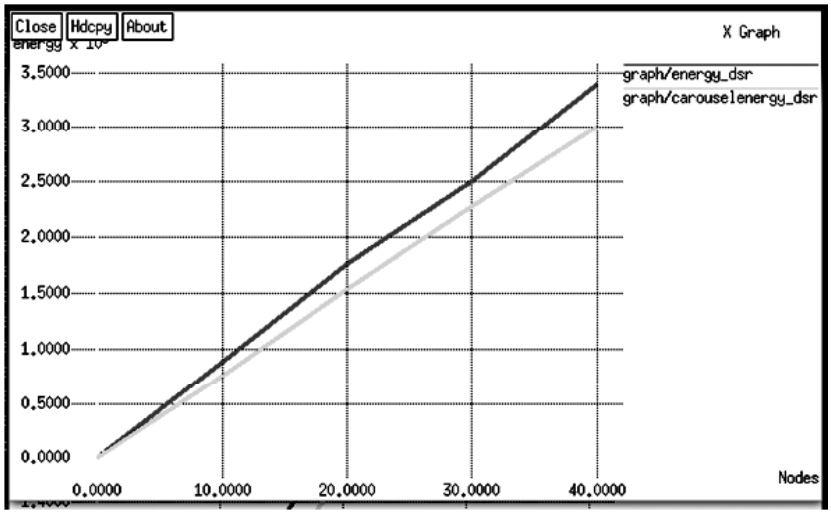

Figure 6: Comparison of remaining energies of DSR and carousel attack on DSR

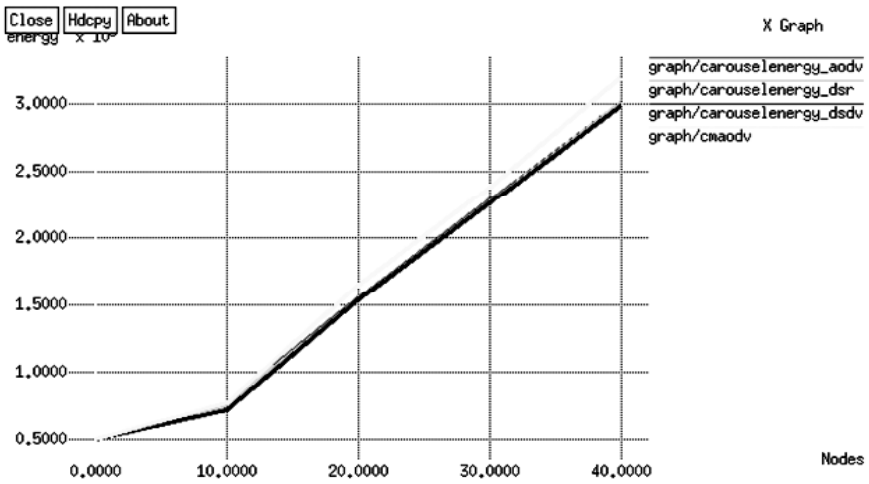

Figure 7: Comparison of remaining energies of carousel AODV, DSDV, DSR and CMAODV

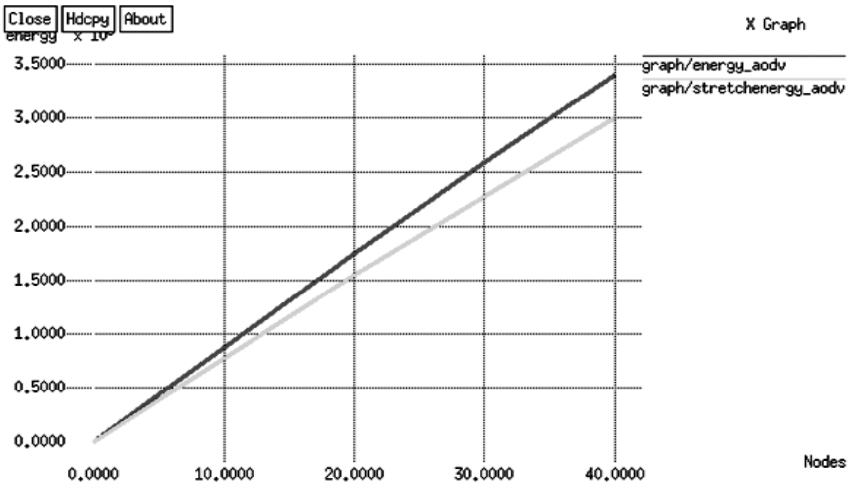

Figure 8: Comparison of remaining energies of AODV and stretch attack on AODV

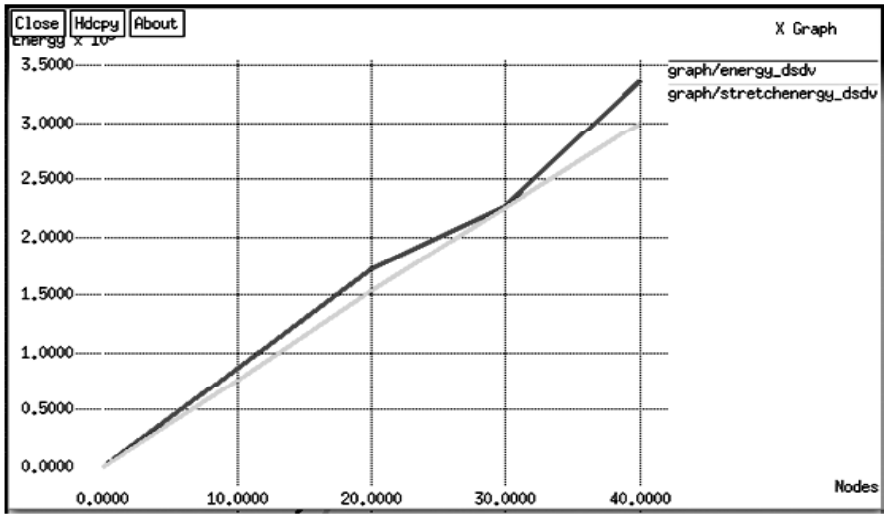

Figure 9: Comparison of remaining energies of DSDV and stretch attack on DSDV

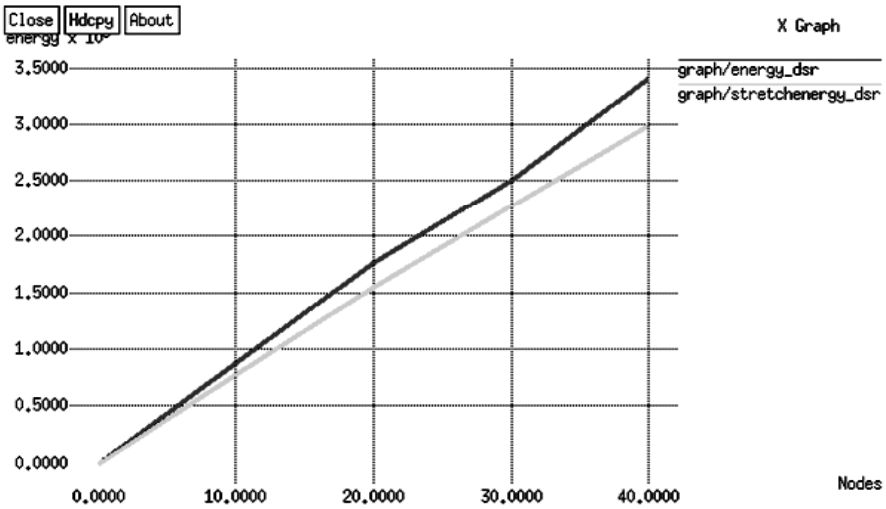

Figure 10: Comparison of remaining energies of DSR and stretch attack on DSR

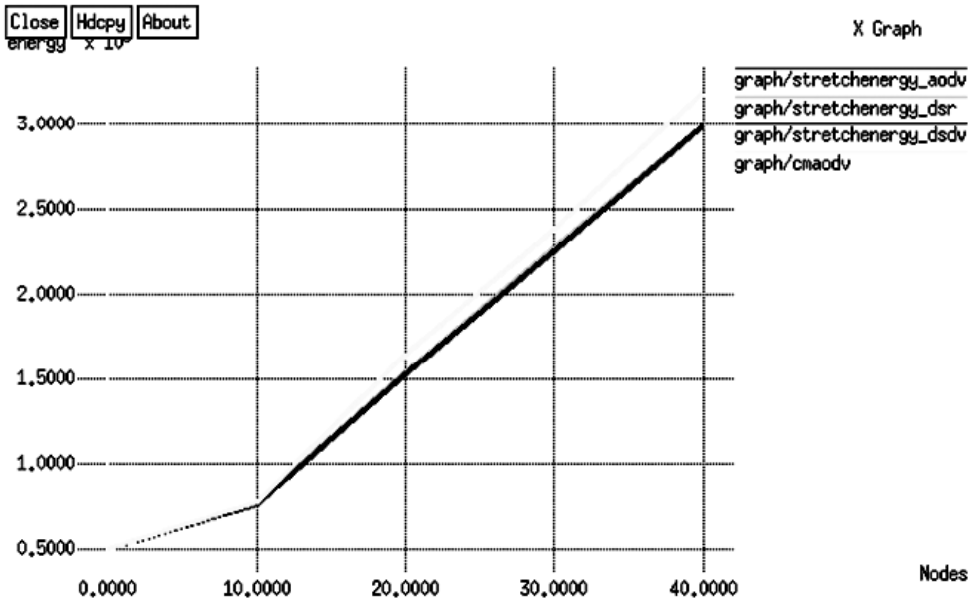

Figure 11: Comparison of remaining energies of stretch AODV, DSDV, DSR and CMAODV

7. CONCLUSION AND FUTURE SCOPE

The research work includes the study of various routing protocols and threats. In this, we discussed detailed research on attacks in MANETs and security issues, and vampire attack which affect the network performance. These attacks uses the routing protocols to permanently disable the network by draining energy of nodes. These attacks are independent on particular protocols or implementation but these shows more vulnerabilities in different protocol classes. Hence there is a need for developing the secure protocols which are not vulnerable to these attacks. The CMAODV works better under attack because the routing in CMAODV is selected based on the cooperative nodes even though the malicious node enter into the network that node need to send the data to next super node by this we can eliminate the loops and long paths in the network .In this method, the energy consumption is normal and also the network is free from attack even though with the presence of malicious node but the attacker node is not identified particularly. With CMAODV the energy loss is reduced since it produces loop free and shortest paths to destination. The vampire attack has very negligible effect on CMAODV. The CMAODV acts as prevention technique to vampire attack.

REFERENCES

Patroklosg. Argyroudis AND Donalo'Mahony "secure routing for mobile ad hoc networks" in IEEE Communication, 2005.

Kejun Liu, Jing Deng, Pramod K. Varshney and KashyapBalakrishnan "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs" in IEEE Transaction, 2007.

Zonghua Zhang, FaridNait-Abdesselam, Pin-Han Ho and Xiaodong Lin "RADAR:aReputAtionbased Scheme for Detecting Anomalous Nodes in WiReless Mesh Networks" in IEEE Communications Society, 2008.

SoufineDjahel, FaridNa¨ıt-Abdesselam and AshfaqKhokhar "An Acknowledgment-Based Scheme to Defend Against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol" in IEEE Communications Society, 2008.

Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour,YoshiakiNemoto and Nei Kato "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks" in IEEE Transactions On Vehicular Technology, 2009.

Zhengming Li, ChunxiaoChigan and Danniel Wong "AWF-NA: A Complete Solution for Tampered Packet Detection in VANETs" in IEEE Communications Society, 2008.

SoufieneDjahel, FaridNait-abdesselam and Zonghua Zhang "Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges" in IEEE Communications Surveys, 2011.

Jin-Hee Cho, Ananthram Swami and Ing-Ray Chen "A Survey on Trust Management for Mobile Ad Hoc Networks" in IEEE Communications Surveys, 2011.

Jian-Ming Chang, Po-Chun Tsou, Han-Chieh Chao and Jiann-Liang Chen "CBDS: A Cooperative Bait Detection Scheme to Prevent Malicious Node for MANET Based on Hybrid Defense.

Architecture" in IEEE Transaction, 2011.

Ian F. Akyildiz, Xudong Wang and Weilin Wang "Wireless mesh networks: a survey" in Science Direct, 2004.

E.A.Mary Anita, V.Thulasi Bai, E.L.Kiran Raj and B.Prabhu "Defending against Worm Hole Attacks in Multicast Routing Protocols for Mobile Ad hoc Networks" in IEEE Transaction, 2011.

Jin Xu "Multicast in Wireless Mesh Networks" in IEEE Transaction. Capkun S., Buttyan L. and Hubaux J. "SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks" in ACM Workshop on Security of Ad Hoc and Sensor Networks (ACM SASN), 2003.

Chiu H. S, Lui K. S. "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks", In International Symposium on Wireless Pervasive Computing. Djenouri D., Khelladi L. and N. Badache "A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks" in IEEE Communication Surveys & Tutorials, 2005.