International Journal of Engineering Science Invention Research & Development; Vol. IV, Issue III, SEPTEMBER 2017
www.ijesird.com, E-ISSN: 2349-6185

SELF-OPTIMIZATION OF HANDOVER PARAMETERS FOR LONG-TERM EVOLUTION WITH DUAL WIRELESS MOBILE RELAY NETWORK

Mangalapudi Vijitha[1], V. Jaikumar[2]
M.Tech (DECS)[1] , Associate Professor[2], Department of ECE, QIS College of Engineering and Technology
Pondur Road, Vengamukkapalem, Ongole- 523272, AP
vijithadeei@gmail.com

Abstract: **Modern years, train passengers comprise been transfer growing amounts of data using mobile strategy. Wireless networks with mobile relay nodes support broadband wireless communications for passengers of such vehicles using backhaul links. conversely, the mobility executive creature reuses the give up of existing user apparatus, resulting in the handover of the Long-Term Evolution network being unsuitable for user equipment within the cabins of vehicles traveling at high speed. We suggest a self-optimizing handover hysteresis method with dual mobile relay nodes for wireless networks in high-speed mobile environments. The future method tunes the hysteresis and unit character offset handover parameters based on the rapidity of the vehicle and the handover performance indicator, which affects the handover triggering decision and performance. The results of simulations conducted in which the performance of the proposed scheme was compared to that of an existing scheme show that the proposed scheme can reduce the number of radio link failures and service interruptions during handover procedures. The challenge is how to prevent these security threats in MANETs. In based on DSR protocol, we propose a detection scheme called the Cooperative Bait Detection Scheme (CBDS), which aims at detecting and preventing malicious nodes launching gray hole/collaborative black hole attacks in MANETs. In this system, it integrates the hands-on and reactive defence architecture and randomly cooperates with a stochastic adjacent node.**

I. INTRODUCTION

Nowadays, Mobile Ad Hoc Network (MANET) has become a practical platform for pervasive social networking and computing, playing as a valuable extension and complement of traditional o n-line social networks over the Internet. For example, a user could query people in vicinity using his/her mobile device about which shop is on sale, which movie is recommended to see, or which mobile application should be installed for tagging the locations of photos. The user neighbours can respond these queries by providing their recommendations via PSN. The users could also chat with people nearby for sharing a taxi ride in a flight before landing or affording the cost of a series of movie tickets in front of a movie theatre. Moreover, they can seek services or aids from strangers in vicinity through PSN. People who are strangers but regularly appear in the same public places could want to make an instant appointment for a face- to-face meeting. Particularly, PSN can be applied to collect useful data about an environment in a pervasive and instant manner. This kind of social networking brings extensive social experiences t o mobile users, thus is very valuable with unlimited potential, especially when the Internet or cellular networks are temporarily unavailable or costly to access. Trust plays an important role in PSN for reciprocal activities among nearby strangers. It is a measure derived from direct or indirect knowledge and experiences based on previous interactions and are used to assess the level of belief and dependence put into an entity. T rust helps people overcome perceptions of uncertainty and risk and engages in “trusted social behaviours". During the instant social activities, users are not necessarily acquaintances but more likely to be strangers. Therefore the users need to balance between the benefits received in such reciprocal activities and the risks related to communications with strangers. In this context, it is important to figure out how much users should trust with each other in order to make a social decision about how to disclose and share personal private information. In order to avoid malicious eavesdropping in PSN, it is crucial to secure PSN communications. It is important to set up a secure communication channel among personally trusted nodes for a serious talk.[1][2][4]

A. BLACK HOLE ATTACK

Black hole attack can be called Packet Drop Attack since it drops many packets. Black hole attack is an active attack. Most frequent attack here is stop forwarding the data packets. If there is a malicious node, it keeps waiting for its neighbour node to initiate RREQ packet. As a node receives the RREQ packet, it will send a false RREP packet instantly with a modified high sequence number. So that the source node will assume that there is a new route is available towards the destination. The source node ignores the RREP packet from the other nodes including the accurate nodes where it automatically denies the other nodes and it will start sending the packets towards the malicious nodes. Then the malicious node takes all the routes towards itself and it doesn't allow forwarding the packets anywhere. This type of attack will happen frequently which is brutal to find out and we use a detection techniques to resolve these attacks. This attack is called a black hole where it consumes all the data. [7][9]

B. GRAY HOLE ATTACK

A variation of black hole attack is the gray hole attack, in which the nodes will drop the packets selectively. Gray hole is a node that can switch from behaving correctly to behaving like a black hole that is it is actually an attacker and it will act as a normal node. So the attacker can't be easily identified since it behaves as a normal node. The address of the adjacent node is used as the bait destination address, baiting malicious nodes to send RREP reply messages and identifies the malicious nodes by using the reverse tracing program. [10][11]

II. EXISTING SYSTEM

DUE to the widespread availability of mobile devices, mobile ad hoc networks (MANETs) have been widely used for various important applications such as military crisis operations and emergency preparedness and response operations. This is primarily due to their infrastructure less property. In a MANET, each node not only works as a host but can also act as a router. While receiving data, nodes also need cooperation with each other to forward the data packets, thereby forming a wireless local area network. These great features also come with serious drawbacks from a security point of view. Indeed, the aforementioned applications impose some stringent constraints on the security of the network topology, routing, and data traffic. For instance, the presence and collaboration of malicious nodes in the network may disrupt the routing process, leading to a malfunctioning of the network operations.

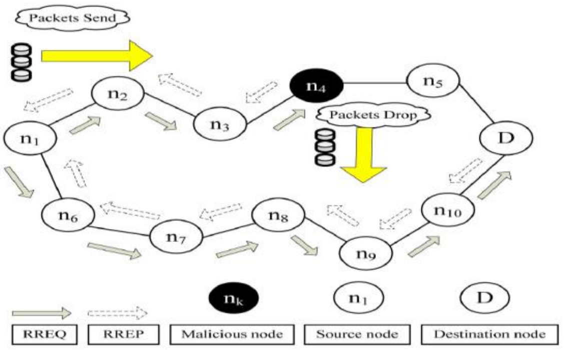


Figure 3.1 Blackhole attack–node n4 drops all the data packets

Many research works have focused on the security of MANETs. Most of them deal with prevention and detection approaches to combat individual misbehaving nodes. In this regard, the effectiveness of these approaches becomes weak when multiple malicious nodes collude together to initiate a collaborative attack, which may result to more devastating damages to the network. The lack of any infrastructure added with the dynamic topology feature of MANETs make these networks highly vulnerable to routing attacks such as blackhole and grayhole (known as variants of blackhole attacks). In blackhole attacks (see Fig. 1), a node transmits a malicious broadcast informing that it has the shortest path to the destination, with the goal of intercepting messages. If an intermediate node has routing information to the destination in its route cache, it will reply with a RREP to the source node. When the RREQ is forwarded to a node, the node adds its address information into the route record in the RREQ packet. When destination receives the RREQ, it can know each intermediary node’s address among the route. The destination node relies on the collected routing information among the packets in order to send a reply RREP message to the source node along with the whole routing information of the established route. DSR does not have any detection mechanism, but the source node can get all route information concerning the nodes on the route. In our approach, we make use of this feature mechanism [so-called cooperative bait detection scheme (CBDS)] is presented that effectively detects the malicious nodes that attempt to launch gray hole/collaborative black hole attacks. [2][3][4]

A. COOPERATIVE BAIT DETECTION SCHEME

Proposes a detection scheme called the cooperative bait detection scheme (CBDS), which aims at detecting and preventing malicious nodes launching gray hole/collaborative black hole attacks in MANETs. In our approach, the source node stochastically selects an adjacent node with which to cooperate, in the sense that the address of this node is used as bait destination address to bait malicious nodes to send a reply RREP message. Malicious nodes are thereby detected and prevented from participating in the routing operation, using a reverse tracing technique. In this setting, it is assumed that when a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node back to the source node to trigger the detection mechanism again. Our CBDS scheme merges the advantage of proactive detection in the initial step and the superiority of reactive response at the subsequent steps in order to reduce the resource wastage. CBDS is DSR-based. As such, it can identify all the addresses of nodes in the selected routing path from a source to destination after the source has received the RREP message. However, the source node may not necessary be able to identify which of the intermediate nodes has the routing information to the destination or which has the reply RREP message or the malicious node reply forged RREP.

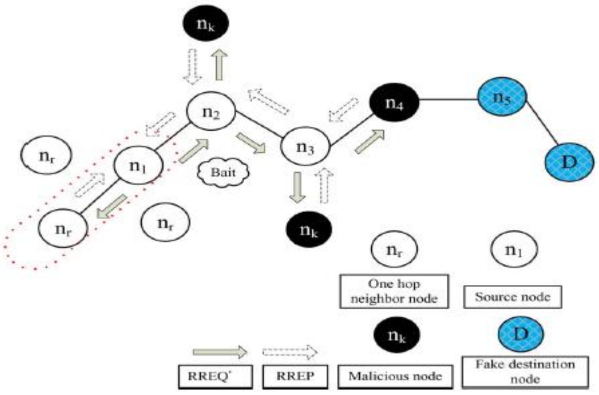


Figure 3.2 Random selection of a cooperative bait address

This scenario may result in having the source node sending its packets through the fake shortest path chosen by the malicious node, which may then lead to a blackhole attack. To resolve this issue, the function of HELLO message is added to the CBDS to help each node in identifying which nodes are their adjacent nodes within one hop. This function assists in sending the bait address to entice the malicious nodes and to utilize the reverse tracing program of the CBDS to detect the exact addresses of malicious nodes. The baiting RREQ packets are similar to the original RREQ packets, except that their destination address is the bait address. The CBDS scheme comprises three steps: 1) the initial bait step; 2) the initial reverse tracing step; and 3) the shifted to reactive defense step, i.e., the DSR route discovery start process. The first two steps are initial proactive defense steps, whereas the third step is a reactive defense step.[5][6]

B. PERFORMANCE METRICS

1) Packet Delivery Ratio:

This is defined as the ratio of the number of packets received at the destination and the number of packets sent by the source. Here, pkt di is the number of packets received by the destination node in the ith application, and pktsi is the number of packets sent by the source node in the ith application. The average packet delivery ratio of the application traffic n, which is denoted by PDR, is obtained as

$$PDR = \frac{1}{n}\sum_{i=1}^{n}\frac{pktd_i}{pkts_i}.$$

2) Routing Overhead:

This metric represents the ratio of the amount of routing-related control packet transmissions to the amount of data transmissions. Here, cpki is the number of control packets transmitted in the ith application traffic, and pkti is the number of data packets transmitted in the ith application traffic. The average routing overhead of the application traffic n, which is denoted by RO, is obtained as

$$RO = \frac{1}{n}\sum_{i=1}^{n}\frac{cpk_i}{pkt_i}.$$

3) Average End-to-End Delay:

This is defined as the average time taken for a packet to be transmitted from the source to the destination. The total delay of packets received by the destination node is *di*, and the number of packets received by the destination node is *pktdi*. The average end-to-end delay of the application traffic *n*, which is denoted by *E*, is obtained as

$$E = \frac{1}{n}\sum_{i=1}^{n}\frac{d_i}{pktd_i}.$$

4) Throughput:

This is defined as the total amount of data (*bi*) that the destination receives them from the source divided by the time (*ti*) it takes for the destination to get the final packet. The throughput is the number of bits transmitted per second. The throughput of the application traffic *n*, which is denoted by *T*, is obtained as

$$T = \frac{1}{n}\sum_{i=1}^{n}\frac{b_i}{t_i}.$$

It can be observed that DSR drastically suffers from blackhole attacks when the percentage of malicious nodes increases.

III. PROPOSED SYSTEM

Proposed a malicious node detection scheme, named as CBDS, which is able to detect and prevent malicious nodes causing black or gray hole attacks and cooperative attacks. It merges the proactive and reactive defense structure, and the source node randomly establishing cooperation with the adjacent node. Using the address of the adjacent node as the destination bait address, it baits malicious nodes to send a RREP reply and detects the malicious nodes by the proposed reverse tracing program and consequently prevents their attacks. We assume that when there is a significant drop in packet delivery ratio, an alarm will be sent by the destination node to the source to trigger the detection mechanism again, which can achieve the capability of maintenance and immediately reactive response. Accordingly, our proposal merges the advantage of proactive detection in the initial stage and the superiority of reactive response that reduce the waste of resource. Consequently, our mechanism doesn't like the method that just use reactive architecture would suffer black hole attack in initial stage. Although DSR can know the all address of nodes among the route after the source node receives the RREP. Nonetheless, the source node cannot identify exactly which intermediate node has routing information to destination node and reply RREP. This situation make the source node sends packets to the shortest path that the malicious node claim and the network suffer black hole attack that causes packet loss. However, the network that uses DSR cannot know which malicious node cause the loss. In comparison to DSR, the function of Hello message like AODV was added to help the nodes to identify which nodes are their adjacent nodes within one-hop. This function assists in sending the bait address to entice the malicious nodes and utilize the reverse tracing program of CBDS to detect the exact addresses of malicious nodes. [2][1]

A. SECURED ROUTING PROTOCOL

The secured routing protocol play important role in mobile ad hoc network. Secured routing protocol defended the attack such as worm whole attack, black hole attack and other internal and external attack. In modification of on-demand routing protocol for prevention of attack, various author are proposed a method such as EAODV (Enhanced on demand distance vector routing protocol) and SBRP (secured backup routing protocol).SBRP is very efficient protocol for secured communication in ad hoc network.

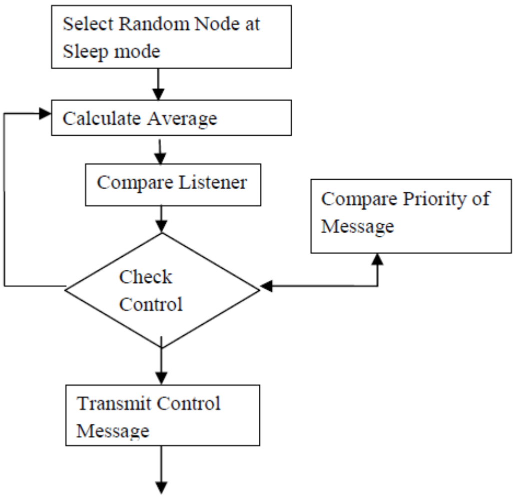


Figure 4- Protocol steps for modified control message protocol

The process of Secured backup routing protocol executes in three phase. (1) Secured route discovery across the node (2) backup node setup (3) route maintenance across the node. The secured process takes time for execution of process of SBRP protocol. The node neighbours a and b are unaware that they have selected by thresholds value. Having observed a collision in its local time t, node w transmits at time t+GA,

B. ALGORITHM FOR DETECTING GRAY/BLACK HOLE

Action by Source Node S
Step 1: Divides the data packets to be sent in k equal parts.
DATA [1,….,K];
Initialize i = 1;
Comment: Chose window size w, If total no of data packets n then k = ceiling (n/w)
Step 2: Send prelude(S,D,ni) message to the destination node D. Where ni is the no of data packets to be sent in current block.
Step 3: Broadcast monitor (S, D, NNR) message to all its neighbors. Instructing neighbors to monitor next node in the route (NNR).
Step 4: Starts transmitting data packets from the block Data[i] to D.
Step 5: Sets timeout TS for the receipt of the postlude (D, S, d_count) message containing d_count, no of data packets received by D.
Step 6: If TS not expired and postlude message received,
if (ni (1−μ)≤ d _ count)
Increment i by 1 and go to Step 8.
else Start Gray/Black hole removal process.
Comment: Where μ is a threshold value ranges between 0 and 1 indicates the fraction of total packets gets lost due to error prone wireless channel. If we assume that μ is the permissible packet loss in each node in the route thenμ = 1− (1−μ)N , where N is the total no of nodes in the route (hop count).
Step 7: If TS expired and postlude message not received then start Gray/Black hole removal process.
Step 8: Continues from Step 2 when i less than equal to k.
Step 9: Terminates S's action. Action by Destination Node D.

C. PERFORMANCE MEASUREMENT OF AD HOC NETWORK

Internet Engineering Task Force (IETF) identified the performance metrics of the ad hoc network based on their behavior. The performance of ad hoc networks based on network capacity, network connectivity, topological change rate, link speed and mobility. The ad hoc network performance measurement is based on the following metrics. Packet transmission ratio: The ratio is measured by number of packets transmitted by source and number of packets received by destination. The measurement is based on Constant Bit Rate (CBR) in order to find out packet loss, throughput of the data in the network. Route procurement time: It mentions the time required to inaugurate the routes. The measurement is based on end system performance. Routing overhead: The routing overhead describes the number of routing packets needed for route discovery and route maintenance phase. It also determines whether the protocol is well situated in low-bandwidth situation and able to work with low power consumption. [5][6]

IV. NETWORK SIMULATOR

A network simulator is a software program that imitates the working of a computer network. In simulators, the computer network is typically modelled with devices, traffic etc and the performance is analyzed. Typically, users can then customize the simulator to fulfil their specific analysis needs.

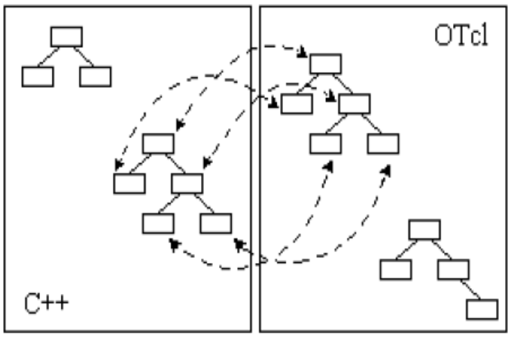


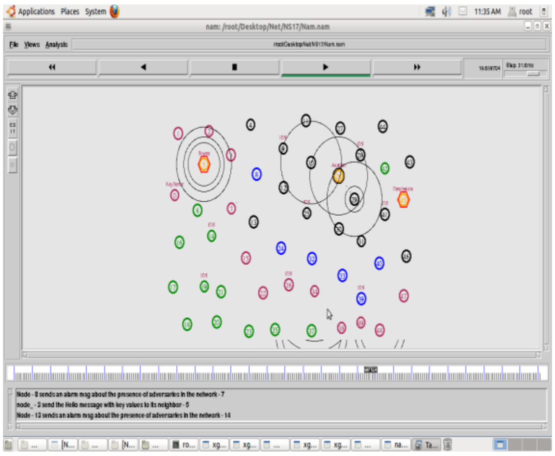
Figure 5. Flow chart for C++ and OTcl

Simulators typically come with support for the most popular protocols in the use today, such as Wireless LAN, Wi-Max, UDP, and TCP. A network simulator is a piece of software or hardware that predicts the behaviour of a network, without an actual network being present. NS is an object oriented simulator, written in C++, with an OTcl interpreter as a frontend. The simulator supports a class hierarchy in C++ and a similar class hierarchy within the OTcl interpreter. The two hierarchies are closely related to each other; from the users perspective, there is one-to-one correspondence between a class in the interpreted hierarchy and one in the compiled hierarchy. The root of this hierarchy is the class Tcl object. Users create a new simulator objects through the interpreter; these objects are instantiated within the hierarchy. The interpreted class hierarchy is automatically established through methods defined in the class Tcl object. There are other hierarchies in the C++ code and OTcl scripts; these other hierarchies are not mirrored in the manner of Tcl object.

A. USES OF NETWORK SIMULATORS

Network simulators serve a variety of needs. Compared to the cost and time involved in setting up an entire test bed containing multiple networked computers, routers and data links, network simulators are relatively fast and inexpensive. They allow engineers to test scenarios that might be particularly difficult or expensive to emulate using real hardware- for instance, simulating the effects of sudden bursts in the traffic or a Dos attack on a network service. Networking simulators are particularly useful in allowing designers to test new networking protocols or changed to existing protocols in a controlled and reproducible environment. Typical network simulators encompasses a wide range of networking technologies and help the users to build complex networks from basic building blocks like variety of nodes and links. With the help of simulators one can design hierarchical networks using various types of nodes like computers, hubs, bridges, routers, optical cross-connects, multicast routers, mobile units, etc. various types of Wide Area Network (WAN) technologies like TCP, ATM, IP etc and Local Area Network (LAN) technologies like Ethernet, token rings etc, can all be simulated with the typical simulator and the user can test, analyze various routing etc.

B. SIMULATION AND RESULTS


Applications Places System
nam: /root/Desktop/Net/NS17/Nam.nam
File Views Analysis

Node - 8 sends an alarm msg about the presence of adversaries in the network - 7
node_ - 3 send the Hello message with key values to its neighbor - 5
Node - 13 sends an alarm msg about the presence of adversaries in the network - 14

Figure 5.3 Communications between Different Types of Nodes

Now present Monte Carlo simulation results of the various algorithms introduced in the paper. The goal of this section is twofold:

- To investigate the performance of these algorithms;
- Use the simulation results to develop a complete BS allocation scheme that indicates when the BS should invoke each algorithm.

Throughout this section, we consider CSI allocation trees whose heights. The average time window between signal-to-interference-plus-noise ratio (SINR) changes is randomly selected between 32 and 1024 subframes. Therefore, for each MS, holds. The average data packet rate for each MS is uniformly chosen between 50 and 1000 packets/s.

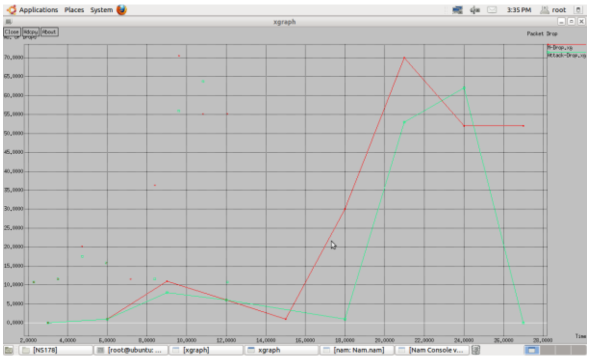


Figure 5.4 Average no of packet drop

In Figure 5.4 shows the –axis indicates the average number of MSs (load) and the -axis indicates the average number of changes per event. The maximum number of changes per event occurs when the average number of MSs is 250, which is expected because, this is where the maximum profit ratio between Algorithms 1 and 2 is obtained. Now show how to adapt the complete BS scheme to the case where the BS has limited CPU resources and is unable to execute both Algorithms 1 and 2 for each event.

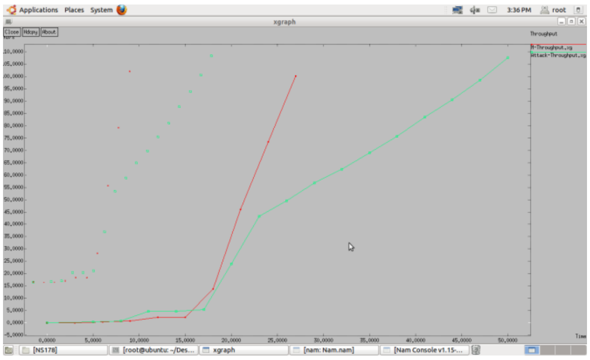


Figure 5.5 Algorithm 1 throughput value

Figure 5.5 shows Algorithms 1 and 2 into a complete allocation scheme for the BS. An action is required from the BS in the following cases: 1) a new MS becomes active; 2) an active MS leaves the cell or becomes inactive; 3) the profit function of an active MS changes (e.g., due to a change in the user mobility speed). Algorithm 2 allows an increase in the profit without the overhead associated with the removal of existing CSI channels. However, Algorithm 2 is often unable to allocate a CSI channel, not because the bandwidth is insufficient, but because it is fragmented.

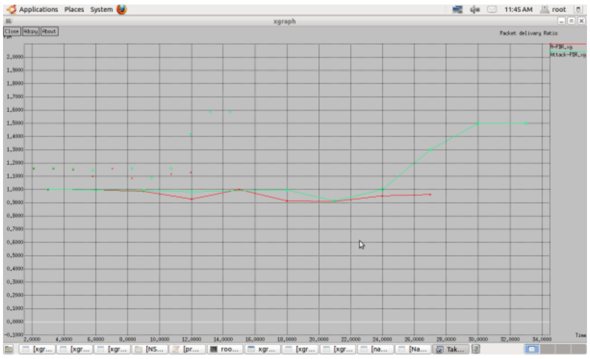


Figure 5.6 Total profit of algorithm 1 & 2

Figure 5.6 shows the cross-layering significantly increases the number of successful join operations, especially in case of very dynamic networks: while the number of successful join operation is consistently above 95% with cross-layering, with the original Chord protocol this percentage can drop to as low as 70% in case of very dynamic networks. We believe this is due to the fact that cross-layering mitigates the negative effects of having inconsistent finger tables, which tend to increase the percentage of unsuccessful join operations. Inconsistencies in the finger tables are clearly more likely to occur under dynamic network conditions, which explains the relatively greater benefits of cross-layering on the percentage of successful join operations under such conditions.

V. CONCLUSION AND FUTURE WORK

General view of multicast routing protocols in ad-hoc networks. Any multicast routing protocol in MANETs tries to overcome some difficult problems which can be categorized under basic issues or considerations. All protocols have their own advantages and disadvantages. One constructs multicast trees to reduce end-to-end latency. Multicast tree-based direction-finding protocols are resourceful and satisfy scalability issue, they have several drawbacks in ad hoc wireless networks due to mobile nature of nodes that participate during multicast session. Multicast mesh of alternate paths between every source-destination pair is established in mesh creation phase. Stable path within a mesh is established by choosing an SFN that possess higher value of link stability among its neighbours. This assures better quality of links and minimizes the possibility of link failures and the overhead needed to construct the paths. In the mesh-based protocols provide more robustness against mobility and save the large size of control overhead used in tree maintenance. Most protocols of this type rely on frequent broadcasting, which may lead to a scalability problem when the number of sources increases. mixture multicast provide which are tree based as well as mesh based and gives the advantage of both types. It is really difficult to design a multicast routing protocol considering all the above mentioned issues. Still it is an open difficulty for researchers to develop a single protocol which can satisfy as many goals as possible in the future.

REFERENCES

[1] P.-C. Tsou, J.-M. Chang, H.-C. Chao, and J.-L. Chen, "*CBDS: A cooperative bait detection scheme to prevent malicious node forMANET based on hybrid defense architecture,*" in Proc. 2nd Intl. Conf. Wireless Commun., VITAE, Chenai, India, Feb. 28–Mar., 03, 2011, pp. 1–5.

[2] S. Corson and J. Macker, RFC 2501, *Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations*, Jan. 1999. (Last retrieved March 18, 2013) Available: http://www.elook.org/computing/rfc/rfc2501.html

[3] C. Chang, Y.Wang, and H. Chao, "*An efficientMesh-based core multicast routing protocol onMANETs,*" J. Internet Technol., vol. 8, no. 2, pp. 229– 239, Apr. 2007.

[4] D. Johnson and D. Maltz, "*Dynamic source routing in ad hoc wireless networks*," Mobile Comput., pp. 153–181, 1996.

[5] I. Rubin, A. Behzad, R. Zhang, H. Luo, and E. Caballero, "*TBONE: A mobile-backbone protocol for ad hoc wireless networks*," in Proc. IEEE Aerosp. Conf., 2002, vol. 6, pp. 2727–2740.

[6] A. Baadache and A. Belmehdi, "*Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks*," Intl. J. Comput. Sci. Inf. Security, vol. 7, no. 1, 2010.

[7] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "*Mitigating routing misbehaviour in mobile ad hoc networks*," in Proc. 6th Annu. Intl. Conf. MobiCom, 2000, pp. 255–265.

[8] K. Vishnu and A. J Paul, "*Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks*," Int. J. Comput. Appl., vol. 1, no. 22, pp. 28–32, 2010.

[9] K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "*An Acknowledgement based approach for the detection of routing misbehavior in MANETs*," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[10] H. Deng, W. Li, and D. Agrawal, "*Routing security in wireless ad hoc network*," IEEE Commun. Mag., vol. 40, no. 10, Oct. 2002.

[11] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "*Prevention of cooperative blackhole attacks in wireless ad hoc networks*," in Proc. Int. Conf. Wireless Netw., Jun. 2003, pp. 570–575.

[12] H. Weerasinghe and H. Fu, "*Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation*," in Proc. IEEE ICC, 2007, pp. 362–367.