A Secure Packet Drop Defense Mechanism in Wireless Mobile Ad-hoc Networks

MUHAMMAD ZAKARYA[1], IZAZ UR RAHMAN[2]

[1]Department of Computer Science, Abdul Wali Khan University, Mardan, **Pakistan**

[2]Department of Information, Computing & Mathematics, Brunel University, **UK**

ABSTRACT. *MANETs have various applications in computer networks, such as providing communication in a domicile lacking network groundwork and proper infrastructure. In MANET, a data packet may crisscross numerous hops until reaching its target location, making it exposed to various networks attacks. The packets in a MANET are exposed to various packet dropping attacks. Due to the absence of a centralized monitoring apparatus, it is one of the most stimulating problems to recognize the attacker. The surviving DoS protective procedures have not provided a structure to proficiently and meritoriously crack this thought-provoking problem. We are going to outline different issues that results in poor QoS and will try to propose a cryptographically secure mechanism to guess the attacker.*

Keywords: MANETs, QoS, DoS, DSR, OLSR, AODV, TORA, CBRP, DSDV, OSPF, FSR, TBRPF, CSGR, ZRP, RREQ, RREP, HM, TC

1. Introduction

MANETs [1, 2, 6, 8, 10, 12, 14] are infrastructure-less, temporary wireless networks, consisting of several stations. No specific topology is defined in MANETs. Mobility is there but security is the main issue still. MANETs are applicable in hazardous area where cabling is an issue, i.e. disaster relief operations, battlefields etc. MANETs have low construction cost and can be build more rapidly as compared to other networks. In these types of networks a node may be a server, a client or it may be a router. A client is requesting for services, server is service provider, and a router is working as a communication point i.e. interconnecting other nodes in the network. The rest of the paper is structured as follows. In section I we give some introduction, II is about related work that we proposed in previous version. We conclude in section VIII, with some future directions and work in subsequent section IX.

2. Routing Protocols:

Routing protocols in MANETs are classified into three different categories [5, 9, 14, 15] according to their functionality.

- Reactive protocols
- Proactive protocols
- Hybrid protocols

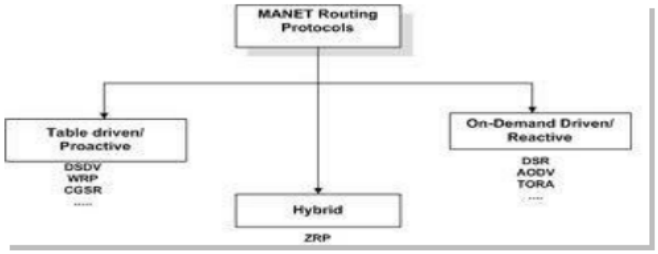


Fig 1: classification of routing protocols

2.1 Reactive Protocols / On demand driven

Reactive protocols are also known as demand driven protocols. In these types of protocols nodes does not initiate rout discovery by themselves whenever they want to communicate with each other. When a source node want to communicate to another node these protocols are responsible to establish rout between these nodes. Some of the major reactive protocols are discussed.

AODV (AD-HOC ON DEMAND DISTANCE VECTOR)

In this routing protocol a node send a RREQ to its neighbors then every neighbor broadcast this packet until the packet reach to its destination when it is received on receiver side the destination send an RREP packet to source node. In this protocol a link has been establish between source and destination and they start communication with each other. If a link is down between two communicating nodes then a RERR packet is generated to inform the source node about break link. I that situation the source node will again broadcast a RREQ packet to establish a new path [47].

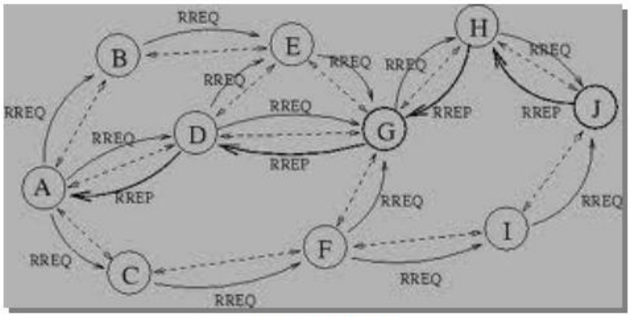


Fig 2: AODV

DSR (DYNAMIC SOURCE ROUTING)

The DSR [50] is an on-demand distance routing protocols that is based on the concept of source routing. Mobile nodes are required to maintain their routing tables that contain source routes from which the mobile node is aware. This protocol consists of two major phases:

a) Rout Discovery, and

b) Rout maintenance.

A mobile node search a rout in the network if it has a rout then it will send the packet if it has no rout then it will establish a rout using the rout discovery method, it will send a packet along with source address to destination. The destination node will reply so that it has established a rout and now it can send data. In rout maintenance whenever a rout link is down an intermediate node will inform the source node that the link has been down, and then the source node will again send a packet to establish a new path.

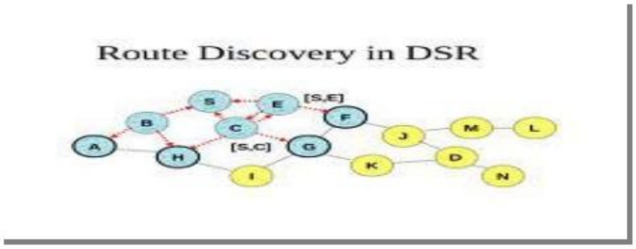


Fig 3: DSR

TORA (TEMPORALLY ORDERED ROUTING ALGORITHM)

The TORA is highly adaptive, scalable, free loop distributed routing algorithm based on the concept of link reversal. TORA is proposed to operate in highly energetic and self-motivated mobile networks. It is source initiated and provides multiple routs for any desired networks. It establishes a rout graph (DAG i.e. Directed Acyclic Graph) between the source node and the destination, the intermediate node comes as well and it record their routing information in its routing table. To accomplish a communication path these nodes needs to maintain routing information about adjacent (one-hope) nodes. This protocol performs three basic functions a) rout creation showing link direction assignment b) rout maintenance showing link reversal phenomenon and c) rout erasure. If a link is break down between the source node and the destination node then the source initiate a new DAG to that specific node [49].

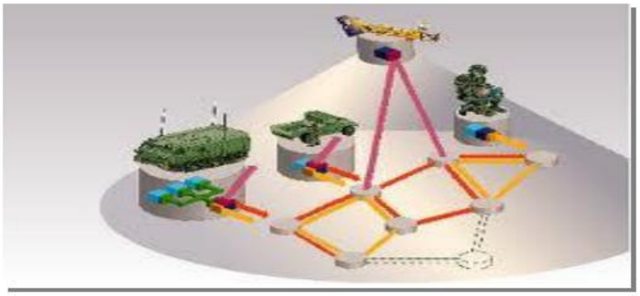
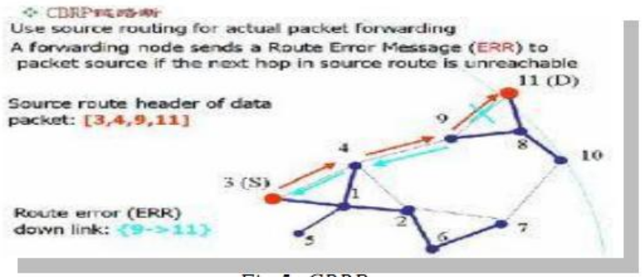


Fig 4: TORA

CBRP (CLUSTER BASED ROUTING PROTOCOL)

CBRP [48] is a steering protocol considered for average to big mobile ad-hoc networks. The set of rules splits the nodes of the ad-hoc network into a number of intersecting or split 2-hop width clusters in a dispersed style. Every group selects a head to recall cluster connection information. The algorithm is a difference of the "lowest ID" group algorithm. The node with a lowest ID between its neighbors is chosen as the Cluster Head (CH). Each node preserves a 381 Neighbor Table and a Group Adjacency Table. Native Table is an abstract facts arrangement that it employs for connection status detecting and cluster development. Group Adjacency Table saves information about head-to-head clusters for Adjacent Cluster Innovation. These tables are restructured by the periodic Hello Messages (HM).



Use source routing for actual packet forwarding

A forwarding node sends a Route Error Message (ERR) to packet source if the next hop in source route is unreachable

Source route header of data packet: [3,4,9,11]

Route error (ERR) down link: {9->11}

Fig 5: CBRP

2.2 PROACTIVE PROTOCOLS / TABLE DRIVEN:

Another type of routing protocols is called proactive protocols. Proactive works another way as compared to reactive protocols, as it maintains the network and make them fully updated about the routing information of the whole network. When there is some change in the network, every node updates them from that and keeps this information in their respective routing tables. Following are some of the major proactive protocols that are implemented in MANETs.

DSDV (DESTINATION SEQUENCE DISTANCE VECTOR)

Destination-Sequenced Distance-Vector (DSDV) Routing [47] is a table-driven routing system for ad-hoc mobile networks built on the Bellman-Ford algorithm. The main influence of the algorithm was to resolve the routing. Each entrance in the routing table holds a classification number, the classification numbers are usually uniform if a link is present; else, an odd number is used. The number is produced by the endpoint, and the emitter wants to send out the next update with this number. Routing material is dispersed between nodes by sending full tips infrequently and smaller incremental updates more regularly.

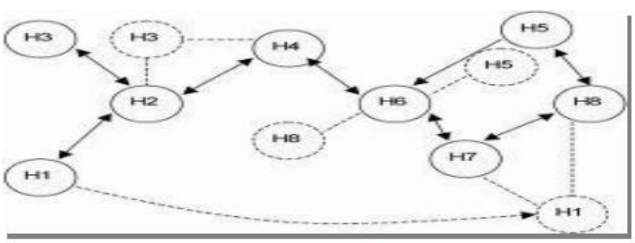


Fig 6: DSDV

OLSR (OPTIMIZED LINK STATE ROUTING)

OLSR is a proactive protocol in which the neighbor’s nodes select an MPR (Multi Point Relay), the unique responsible for spreading the local link information to whole network. It forward its neighbor packets to another node to which it want to communicate. In OLSR every node periodically send a TC (Topology Control) message to whole network to get update information about the network. The MPR selection is based on the willingness of that node (selected MPR) and its response time [46].

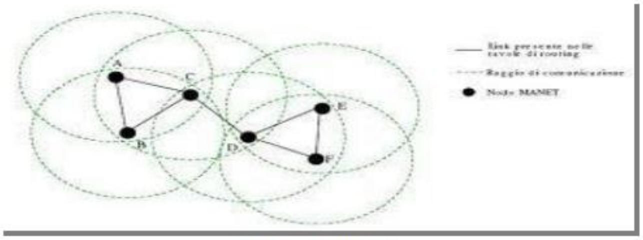


Fig 7: OLSR

OSPF (OPEN SHORTEST PATH FIRST)

OSPF is an internal doorway protocol that routes Internet Protocol (IP) sachets exclusively within a single routing area (autonomous system). It racks link state information from existing routers and builds a topology map of the network. The topology regulates the routing table offered to the Internet Layer which makes routing choices based exclusively on the endpoint IP address found in IP packets. OSPF was planned to support variable-length subnet masking (VLSM) or Classless Inter-Domain Routing (CIDR) talking replicas. OSPF senses changes in the topology, such as link letdowns very rapidly and converges on a new loop-free routing structure within seconds. It calculates the shortest path tree for each route using a method based on Dijkstra's algorithm i.e. a shortest path algorithm [45].

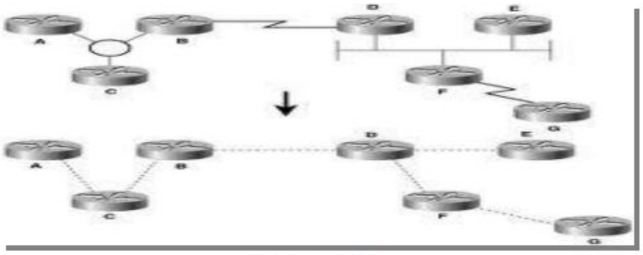


Fig 8: OSPF

FSR (FISHEYE STATE ROUTING)

FSR [44] is an understood ranked routing protocol. It uses the “fisheye” method planned by Klein rock and Stevens, where the technique was used to decrease the size of information compulsory to signify graphical facts. The eye of a fish captures with high aspect the pixels near the focal point. The detail declines as the distance from the focal point increases. In routing, the fisheye approach decodes to preserving correct distance and path class information about the instant region of a node, with increasingly less aspect as the remoteness increases. FSR is functionally alike to LS Routing in that it upholds a topology map at each node. The key change is the way in which routing information is dispersed. In LS, link state packets are produced and drowned into the network whenever a node senses a topology alteration. In FSR, link state packets are not drowned. In its place, nodes keep a link state table built on the up-to-date information acknowledged from near nodes, and intermittently exchange it with their local neighbors only (no drowning). Through this exchange process, the table records with higher sequence numbers swap the ones with lesser sequence numbers. The FSR periodic table interchange resembles the vector interchange in Distributed Bellman-Ford (DBF) (or more precisely, DSDV) where the remoteness are updated according to the time brand or sequence number allocated by the node creating the update. However, in FSR link conditions rather than distance vectors are broadcasted. Moreover, like in LS, a full topology map is kept at each node and shortest paths are calculated using this map.

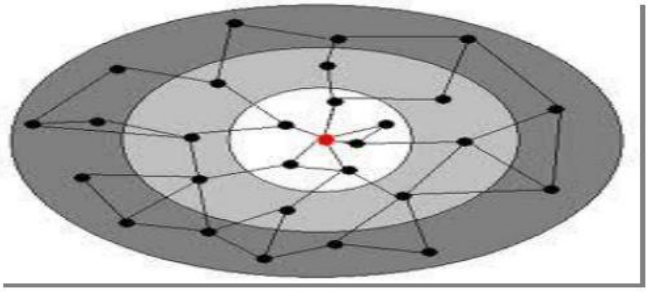


Fig 9: FSR

TBRPF (TOPOLOGY BROADCAST BASED ON REVERES PATH FORWARDING)

TBRPF [43] is a proactive, link-state routing protocol planned for mobile ad-hoc networks, which delivers hop-by-hop routing along with shortest paths to each endpoint. Each node running TBRPF calculates a source tree (providing paths to all reachable nodes) built on fractional topology information kept in its topology table, using an alteration of Dijkstra's algorithm. To reduce overhead, each node reports only portion of its source tree to neighbors. TBRPF uses a mixture of periodic and differential updates to keep all neighbors informed of the stated part of its source tree. Each node also has the option to report supplementary topology information (up to the full topology), to deliver better forcefulness in highly mobile networks. TBRPF achieves neighbor detection using "variance" HELLO messages which report only fluctuations in the status of neighbors. This outcome in HELLO messages that are much lesser than those of other link-state steering protocols such as OSPF.

CSGR (CLUSTER SWITCH GATEWAY ROUTING)

A Cluster Switch Gateway Routing protocol is a proactive protocol in which the mobile nodes are grouped into cluster and each cluster has a cluster head. The cluster head control a group of ad-hoc nodes and it provide a framework for code separation amongst the clusters, channel access routing and bandwidth allocation. To select a cluster among them, distributed cluster head algorithm is used. It controls and coordinates other nodes in that cluster. When a cluster head moves away a new cluster head must be selected. This can be problematic because if a cluster is selected and it moves from that cluster then the network select another node as a cluster head and it is time-consuming as well as. If it reselect the cluster again and again so they will never forward any message to other clusters or nodes. To reduce this overhead a Least Cluster Change (LCC) algorithm is used, using the LCC a cluster head changes only when two cluster head come into contacts, or when a node moves out of all other cluster head [42].

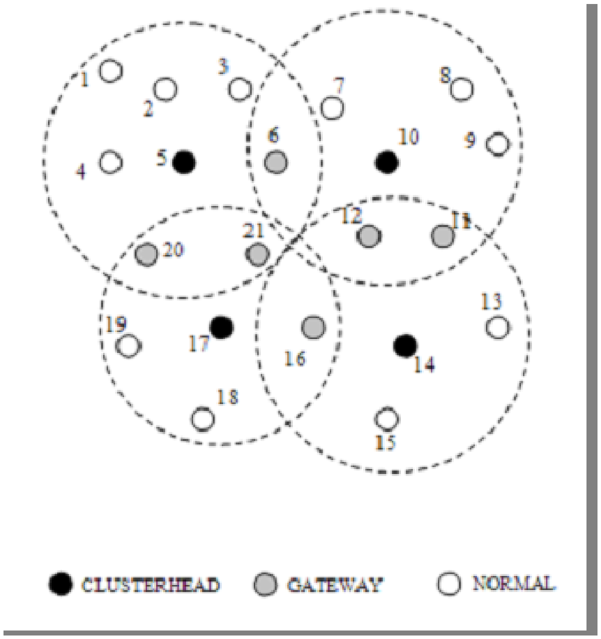


Fig 10: CSGR

HYBRID PROTOCOLS:

Hybrid protocol is the combination of reactive protocols and proactive protocols. The functionality of both reactive and proactive is involved in hybrid protocols. Nodes are connected in zones so the connectivity between nodes is providing by reactive protocols while the connectivity of two zones is provide by proactive protocols.

ZRP (ZONE ROUTING PROTOCOL)

ZRP [41] was the leading hybrid routing protocol with both a preemptive and a responsive routing section. ZRP was planned to decrease the organized overhead of upbeat routing protocols and discount the latency affected by route detection in reactive routing protocols. ZRP defines a region round each node containing of the node's k-neighborhood (that is, all nodes inside k hops of the node). Proactive, Intra-zone Routing Protocol (IARP) is recycled inside routing zones, and a reactive routing protocol, Inter-zone Routing Protocol (IERP), is used amongst routing zones. A route to a terminus inside the native zone can be recognized from the basis's proactively collected routing table by IARP. So, if the basis and terminus of a sachet are in the similar zone, the sachet can be provided immediately. Most of the current proactive routing algorithms can be recycled as the IARP for ZRP.

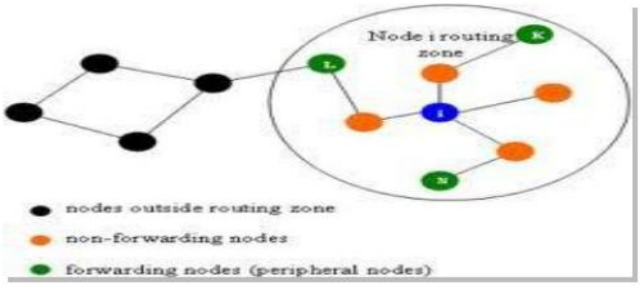

Node i routing zone
K
L
i
N
nodes outside routing zone
non-forwarding nodes
forwarding nodes (peripheral nodes)

Fig 11: ZRP

3. Comparative Study

Reactive protocols are mostly flat in routing structure, hybrid are hierarichal while proactive might be flat and/or hierarichal. Route is always available in proactive protocols while in reactive route is available on demand. Similarly traffice volume is high in proactive, lower in reactive and is lowest in hybrid nature routing protocols. The following section summarize some of the routing protocols and compares then for QoS [51].

	DSDV	**AODV**	**DSR**	**OLSR**	**ZRP**
Multicast routing	No	No	Yes	Yes	No
Type	Distributed	Distributed	Distributed	Distributed	Centralized
Periodic broadcast	Yes	Yes	No	Yes	No
QoS support	No	No	No	Yes	No
Communication overhead	Low	Low	Average	High	Average
Rout metric	Shortest path	Shortest path	Shortest path	Shortest path	Shortest path
Routing table	Yes	Yes	No	Yes	No
Route cache	No	No	Yes	No	Yes
Routing structure	Flat	Flat	Flat	Flat	Flat
Hello message	Yes	Yes	No	Yes	Yes

Table 1. Comparative Study DSDV, AODV, DSR, OLSR, ZRP

	TORA	**ABR**	**LSR**	**SLR**	**GRP**
Multicast routing	Yes	No	Yes	Yes	Yes
Type	Distributed	Local broadcast	Distributed	Distributed	Centralized
Periodic broadcast	Yes	Yes	Yes	Yes	No
QoS support	Yes	Yes	No	Yes	No
Communication overhead	High	Average	High	High	High
Rout metric	Shortest path	Strongest associativity	RRL	Shortest path	Shortest path
Routing table	Yes	Yes	Yes	No	No
Route cache	No	No	No	Yes	Yes
Routing structure	Flat	Flat	Flat	Flat	Hierarchal
Hello message	No	Yes	No	Yes	No

Table 2. Comparative Study TORA, ABR, LSR, SLR, GRP

	R-DSDV	**H-OLSR**	**GSR**	**Q-OLSR**	**WRP**
Multicast routing	Yes	No	Yes	Yes	Yes
Type	Distributed	Local broadcast	Distributed	Distributed	Centralized
Periodic broadcast	Probabilistic	Yes	Yes	Yes	Yes
QoS support	Yes	Yes	Yes	Yes	No
Communication overhead	Low	High	Low	High	Low
Rout metric	Shortest path	Shortest path	Shortest path	No	Shortest path
Routing table	Yes	Yes	Yes	Yes	Yes
Route cache	No	No	No	No	No
Routing structure	Hierarchal	Hierarchal	Flat	Flat	Flat
Hello message	Yes	No	No	No	Yes

Table 3. Comparative Study R-DSDV, H-OLSR, GSR, Q-OLSR, WRP

	FSR	DDR	DST	ANSI	FZRP
Multicast routing	No	No	Yes	Yes	No
Type	Distributed	Local broadcast	Distributed	Distributed	Centralized
Periodic broadcast	Probabilistic	Yes	Yes	Yes	Yes
QoS support	Yes	No	Yes	No	No
Communication overhead	Low	Low	Low	Average	Average
Rout metric	Scope range	Stable routing	No	Shortest path	Shortest path
Routing table	Yes	No	Yes	Yes	No
Route cache	No	Yes	No	No	Yes
Routing structure	Flat	Hierarchal	Hieratical	N/A	Flat
Hello message	No	Yes	No	N/A	Yes

Table 4. Comparative Study FSR, DDR, DST, ANSI, FZRP

4. Existing Problem

The packets in a MANET are exposed to various packet dropping attacks. Due to the absence of a centralized monitoring apparatus, it is one of the most stimulating problems to recognize the attacker. The surviving DoS protective procedures have not provided a structure to proficiently and meritoriously crack this thought-provoking problem. We in this article are going to propose a cryptographically secure mechanism to trace the attacker.

5. Proposed Work

Although a lot of protocols are planned for MANET'S on which nodes are interconnected with each other and the data are shifted from one node to alternative node precisely and necessity. Although it reaches securely but all of these mechanisms has more advantages but it have a lot of drawbacks as well. In this paper we have introduce a secure mechanism to for routing in MANET'S to dash the node who interrupt the network communication between the nodes which is called a MALICIOUS or SELFISH nodes. The difference between the selfish and a malicious node is that a malicious node have used its resources to drop a packet while a selfish node don't used its resources and drop the packet to break the communication they save their resources to forward their own packets. Our focus is on that both intruders that are "trace the guy who killed the network traffic". It means that how we can trace the node that disturbed the network communication by dropping the data packets as well as the control messages. The solution which we have proposed is NHNI (Next Hope Neighbor Investigation). In this protocol we investigate the next neighbor of the node for the purpose of the receiving the packet or not. For this the source node first establishes the rout using any of the proposed rout discovery protocol. When the path is established between the sender and the receiver then the source node will send a data packet to destination node. After sending packet the sender sends an investigation packet (which include a question that is "have you received the data packet") on another shortest route to the receiver. When the destination receives this packet, they will answer that packet and send it back to the source node. If the destination node answered yes "I have received data packet", the communication will continue between the source node and the destination node otherwise if the answer become "NO" from the destination, then the source node will knew that there is a problem in the rout so they will begin the investigation process from the next hope neighbor. They will send an investigation packet to next hope neighbor and again they will ask that question that is data packet received by that if the answer is "YES" then it means that the packet has been received by this node and they didn't forward that so the malicious node is that node if the node answer "NO" so the source node investigate next node and it will continue the process until it didn't find the malicious node.

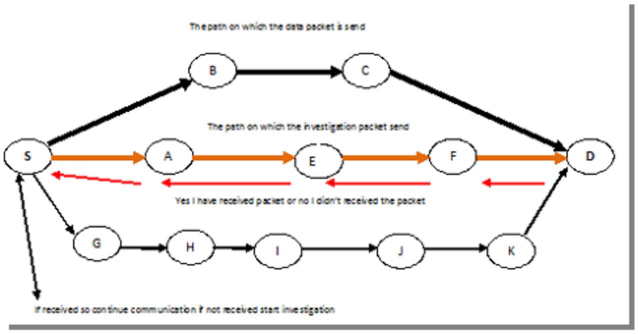

The path on which the data packet is send
B
C
The path on which the investigation packet send
S
A
E
F
D
Yes I have received packet or no I didn't received the packet
G
H
I
J
K
If received so continue communication if not received start investigation

Fig 12: Proposed Scheme

In figure 12 the sender node "S" send the data packet to destination "D" on shortest route which is selected by using any of routing algorithm in that path the node are present that is "B" and "C" which agreed that It will forward the packet of "S" to "D" the destination will receive that packet in a specific time period and it will response to source that either it has received the packet or not if the packet received by the destination and it acknowledged accurate to the source node so that's fine it will communicate with each other but if the destination node didn't responded then the source node will send an investigation packet to the receiver on another selected path in the network the investigation packet include a question that is "did you received the packet or not" if it answered NO so the source node will investigate the next neighbor node that is “C”.

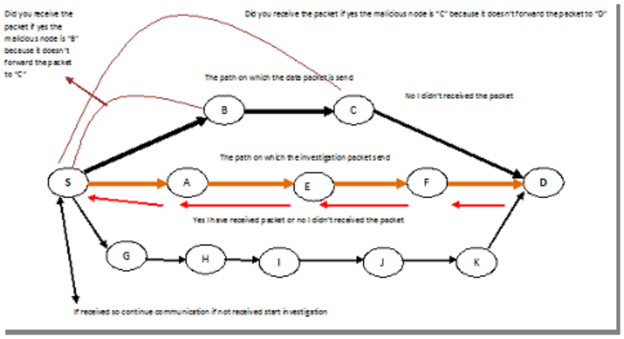

Did you receive the packet if yes the malicious node is "B" because it doesn't forward the packet to "C"
Did you receive the packet if yes the malicious node is "C" because it doesn't forward the packet to "D"
The path on which the data packet is send
No I didn't received the packet
B
C
The path on which the investigation packet send
S
A
E
F
D
Yes I have received packet or no I didn't received the packet
G
H
I
J
K
If received so continue communication if not received start investigation

Fig 13: Working Diagram

When the node “C” received the investigation packet it will must answered that if it answer is “YES” then the source node will know that the malicious node is “C” because it doesn’t forward the packet to node “D” which is destination node. And if it answered “NO” then the source node will investigate the next node which “B” again same question will be asked from “B” if it answered “YES” then the malicious node is “B” because it didn’t forward the packet to “C”.

6. Conclusion

MANETs are infrastructure-less, temporary wireless networks, consisting of several stations [30, 31, 32]. No specific topology is defined in MANETs. Mobility is there but security is the main issue still. One of the major research issues i.e. packet dropping is considered in this article. The packets in a MANET are exposed to various packet dropping attacks. Due to the absence of a centralized monitoring apparatus, it is one of the most stimulating problems to recognize the attacker. In this paper we proposed a new packet dropping technique for tracing the attacker in MANETs. A number of latest research articles were studied. To the best of our knowledge, we found no efficient solution to the problem. The proposed scheme is not implemented and is under consideration for simulation in NS2.

7. Future Work

Security [19, 20, 21, 22] and power consumptions [24, 25, 26, 27, 29, 39, 40] are a widespread problems that has not been overlooked by service discovery protocols. We in this paper did not discuss any security or power consumption issue. Sometimes this issue is so important that is part of the main design strategies. Major security constraints include authentication, authorization, trust, confidentiality, integrity, and non-repudiation. Our future work includes security in service discovery in MANETs. With the rise of new computing era i.e. green computing, there is a need to reduce the power consumption of mobile devices to extend its battery life, as these devices are battery operated. The underlying communication protocols are needs to be less power consumption and more reliable [36, 38]. Our future work is whenever the malicious node is traced then a specific algorithm is needed to block the malicious node or blame it or to fix a black label on it from which it will be excluded out from the network and whenever it join another network so the nodes of that network will know that it is a malicious node which is excluded from another network.

References

[1] Tsu-Wei Chen. "Fisheye state routing: a routing scheme for ad hoc wireless networks", 2000 IEEE International Conference on Communications ICC 2000 Global Convergence through Communications Conference Record ICC-00, 2000

[2] Christos Zaroliagis. "Routing protocols for efficient communication in wireless ad-hoc networks", Proceedings of the 3rd ACM international workshop on Performance evaluation of wireless ad hoc sensor and ubiquitous networks - PE-WASUN 06 PE-WASUN 06, 2006

[3] Pavan Kumar Ponnapalli. "Wireless Mesh Networks: Routing Protocols and Challenges", Communications in Computer and Information Science, 2010

[4] David A. Sumy. "An Overview of Routing Protocols for Mobile Ad Hoc Networks", Ultra Wideband Wireless Communication, 09/09/2006

[5] Nadia N. Qadri. "Analysis of Pervasive Mobile Ad Hoc Routing Protocols", Computer Communications and Networks, 2009

[6] Mohamed Aissani. "Link failure resilience in the dynamic source routing protocol", Wireless Communications and Mobile Computing, 2008

[7] Jyu-Wei Wang. "A Secure DSDV Routing Protocol for Ad Hoc Mobile Networks", 2009 Fifth International Joint Conference on INC IMS and IDC, 08/2009

[8] Mohd Hairil Fitri Ja'afar. "Mobile ad hoc network overview", 2007 Asia-Pacific Conference on Applied Electromagnetics, 12/2007

[9] Suparna DasGupta. "LORP: Least Overhead Routing Protocol for MANET", 2010 International Conference on Wireless Communication and Sensor Computing (ICWCSC), 01/2010

[10] Wang, N.C.. "A stable weight-based on-demand routing protocol for mobile ad hoc networks", Information Sciences, 20071215

[11] Wen Zeng. "A Reliable Routing Protocol for Multi-Hop Ad Hoc Networks", 2007 International

Conference on Wireless Communications Networking and Mobile Computing, 09/2007

[12] K. Gopalakrishnan. "Collaborative Polling based Routing Security Scheme to Mitigate the Colluding Misbehaving Nodes in Mobile Ad Hoc Networks", Wireless Personal Communications, 10/12/2011

[13] N. Sengottaiyan. "A Hybrid Routing Protocol for Wireless Sensor Network", Communications in Computer and Information Science, 2010

[14] Li-Pin Tseng Chun-Chuan Yang. "Fisheye zone routing protocol for mobile ad hoc networks", Second IEEE Consumer Communications and Networking Conference 2005 CCNC 2005, 2005

[15] C.-K. TOH, Adhoc Mobile Wireless Networks, Protocols and Systems, Pearson, Low Price Edition

[16] Ma. Ke, Yu. Nenghai, Liu. Bin, A new packet dropping policy in delay tolerant network, IEEE 2010

[17] Ling Shi, Li Qiu, State Estimatio Over a Network: Packet-dropping Analysis and Design, IEEE 2009

[18] Soufiene Djahel, Farid Nait-abdesselam, Zonghua Zhang, Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges, IEEE 2011

[19] Muhammad Zeshan, Shoab A.Khan, Ahmed Raza Cheema, Attique Ahmed, Applying Security against Packet Dropping Attack in Mobile Ad Hoc Networks, IEEE 2008

[20] Pekka Nikander, Jari Arkko, Toumas Aura, Gabriel Montenergo, Mobile IP version 6 (MIPv6) Route Optimization Security Design, Erricsson Research Nomadic Lab Finland

[21] Wei-Cheng Xiao, Lei Tang, COMP 527 Final Project Report

[22] Sukla Banerjee, Detection / Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks, WCECS 2008

[23] Christopher N. Ververidis, George C. Polyzos, Service Discovery for Mobile Ad Hoc Networks: A Survey of Issues and Techniques, IEEE 2008

[24] Zakarya, M., & Khan, A. A. (2012). Cloud QoS, High Availability & Service Security Issues with Solutions. *IJCSNS*, *12*(7), 71.

[25] M. Zakarya, A.A. Khan, H. Hussain, “Grid High Availability & Service Security Issues with Solutions”, ICIIT 2010, 978-1-4244-813 8-5/10 / $ 26.00 C 2010 IEEE

[26] Zakarya, M., & Afzal, S. (2013). DDoS Confirmation & Attack Packet Dropping Algorithm in On-Demand Grid Computing Platform. *VAWKUM Transaction on Computer Sciences*, *1*(1).

[27] Zakarya, M., Khan, A. A., & Hussain, H. (2010). Grid High Availability and Service Security Issues with Solutions

[28] Cheng, L. (2002, November). Service advertisement and discovery in mobile ad hoc networks. In *Proc. of CSCW*.

[29] Zakarya, M. (2013). SMART GRIDS: A prologue & unscrew challenges that needs to be addressed, A Short Survey on how to make Grids Smarter.*VAWKUM Transaction on Computer Sciences*, *1*(1).

[30] Kozat, U. C., & Tassiulas, L. (2004). Service discovery in mobile ad hoc networks: an overall perspective on architectural choices and network layer support issues. *Ad Hoc Networks*, *2*(1), 23-44.

[31] Lee, C., & Helal, S. (2002). Protocols for service discovery in dynamic and mobile networks. *International Journal of Computer Research*, *11*(1), 1-12.

[32] Zakarya, M., Shah, S. B. H., Alam, A., ur Rahman, A., & ur Rahman, A. (2011). An Overview of New Ultra Lightweight RFID Authentication Protocol SASI.

[33] Bettstetter, C., & Renner, C. (2000, September). A comparison of service discovery protocols and implementation of the service location protocol. In*Proceedings of the 6th EUNICE Open European Summer School: Innovative Internet Applications*.

[34] Mian, A. N., Baldoni, R., & Beraldi, R. (2009). A survey of service discovery protocols in multihop mobile ad hoc networks. *Pervasive Computing, IEEE*,*8*(1), 66-74.

[35] Zakarya, M., Rahman, I., & Ullah, I. (2012). An Overview of File Server Group in Distributed Systems.

[36] Sailhan, F., & Issarny, V. (2005, March). Scalable service discovery for MANET. In *Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on* (pp. 235-244). IEEE.

[37] Zakarya, M., Rahman, I. U., Dilawar, N., & Sadaf, R. An integrative study on bioinformatics computing concepts, issues and problems. *International Journal of Computer Science (IJCSI)*, *8*(6).

[38] Meyer, D., & Fenner, B. (2003). Multicast source discovery protocol (MSDP).

[39] Zakarya, M., Dilawar, N., Khattak, M. A., & Hayat, M. (2013). Energy Efficient Workload Balancing Algorithm for Real-Time Tasks over Multi-Core. *World Applied Sciences Journal*, *22*(10), 1431-1439.

[40] Khan, A. A., & Zakarya, M. (2010). PERFORMANCE SENSITIVE POWER AWARE MULTIPROCESSOR SCHEDULING IN REAL-TIME SYSTEMS.*Technical Journal UET Taxila (Pakistan)*

[41] Haas, Z. J., Pearlman, M. R., & Samar, P. (2002). The zone routing protocol (ZRP) for ad hoc networks.

[42] Sari, R. F., Syarif, A., Ramli, K., & Budiardjo, B. (2005, November). performance evaluation AODV routing protocol on ad hoc hybrid network testbed using PDAs. In *Networks, 2005. Jointly held with the 2005 IEEE 7th Malaysia International Conference on Communication., 2005 13th IEEE International Conference on* (Vol. 1, pp. 6-pp). IEEE.

[43] Ogier, R., Templin, F., & Lewis, M. (2004). *Topology dissemination based on reverse-path forwarding (TBRPF)*. RFC Editor.

[44] Pei, G., Gerla, M., & Chen, T. W. (2000). Fisheye state routing: A routing scheme for ad hoc wireless networks. In *Communications, 2000. ICC 2000. 2000 IEEE International Conference on* (Vol. 1, pp. 70-74). IEEE.

[45] Pióro, M., Szentesi, A., Harmatos, J., Jüttner, A., Gajowniczek, P., & Kozdrowski, S. (2002). On open shortest path first related network optimisation problems. *Performance Evaluation*, *48*(1), 201-223.

[46] Clausen, T., Jacquet, P., Adjih, C., Laouiti, A., Minet, P., Muhlethaler, P., ... & Viennot, L. (2003). Optimized link state routing protocol (OLSR).

[47] Perkins, C. E., & Royer, E. M. (1999, February). Ad-hoc on-demand distance vector routing. In *Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99. Second IEEE Workshop on* (pp. 90-100). IEEE.

[48] Manjeshwar, A., & Agrawal, D. P. (2001, April). TEEN: ARouting Protocol for Enhanced Efficiency in Wireless Sensor Networks. In *IPDPS* (Vol. 1, p. 189).

[49] Park, V. D., & Corson, M. S. (1998, July). A performance comparison of the temporally-ordered routing algorithm and ideal link-state routing. In *Computers and Communications, 1998. ISCC'98. Proceedings. Third IEEE Symposium on*(pp. 592-598). IEEE.

[50] Johnson, D. B., Maltz, D. A., & Broch, J. (2001). DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks. *Ad hoc networking*, *5*, 139-172.

[51] Mehran Abolhasan, Tadeusz Wysocki, Eryk Dutkiewicz, A review of routing protocols for mobile adhoc networks, 2003 Elsevier B.V. All rights reserved. doi: 10.1016/S1570-8705(03)00043-X