JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

New Secure Communication Framework for Detection, Prevention & Isolation of Malicious Modes in MANET

Priya[1*], Yogesh Kumar[2], Rahul Rishi [3]

[1] UIET, MD University, Rohtak, India
[2] UIET, MD University, Rohtak, India
[3] UIET, MD University, Rohtak, India

*Corresponding Author: pg.16594@gmail.com, Tel.: +91-90345-56868

Available online at: www.ijcseonline.org

Accepted: 10/Jul/2018, Published: 31/Jul/2018

Abstract— An ADHOC arranges is an accumulation of remote portable hubs or hosts framing an impermanent system without necessity of any settled framework. In such a domain, to forward a packet from source host to goal have require an on-way host to forward information bundles. ADHOC frameworks rely upon multi-hop guiding from a source to an objective center point or centers. These frameworks have various impediments in light of helplessness of radio interface and its requirements .Problems faced by communication system due to lack security, Attacks has shown that if security is not included in the basic system at the beginning stage, then malicious nodes/users would exploit in the network. With this research work, New Security framework for prevention from suspicious nodes in the mobile ADHOC network is represented. This new security framework will contain efficient approach that will detect, isolate and prevent data from suspicious node by using scattering techniques. This will lead us to propose new security in MANET communication.

***Keywords* —** MANET, Wireless Network, Protocol, Secure Communication, Security

I. Introduction

In MANET, Advancement of routing will provide support for scaling of dynamic hubs. Proactive and Reactive protocols are determining in gathering of routing protocol in MANET. Figure 1 speaks to the classification in routing protocol. In proactive, hub send information to other hub, however if there should arise an occurrence of protocols, the issue happen because of energy devoured and traffic activity. Utilization of local assets additionally happens. Every last hub keeps up routing table with Update of table to store information or data. Table driven protocols incorporate WRP, DSDV. Reactive protocols will found a course, whereby, a host will convey and has data to send. [1-4].

Versatility diminishes the execution in the both types of protocols. In this, routing protocol need to discover over and over new course for better data packet transmission to the goal, because of portability, hub can't be discovered this will emerge to the issue of unpredictability by this hub needs to hold up until the point when another course is found to the goal.[2][4]

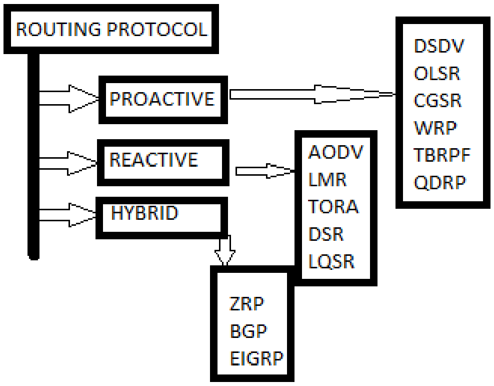


Figure 1: Routing Protocols

II. Attacks On Manet

As of late, numerous conceivable uses of ADHOC systems are talked about, for example, in sensor systems, gathering meeting and reaching out of the scope of base station using specially appointed systems. In these applications, the hubs don't generally have a place with one proprietor OR offer normal goal, subsequently hubs may not will to course parcels for different hubs for different reasons. These reasons can incorporate business advantages or it might need to safeguard its own particular battery life. [4][5]

Because of the idea of the remote medium, malicious hubs, which may not have a place with any association, can upset the tasks of specially appointed systems by infusing incorrectly routing data or infusing modified information packets. Also, infections can disturb the activities of systems by adjusting the conduct of routing protocols or denial of service attack by sending substantial number of modified routing or information packets into the systems.

Current plans of identifying hub trouble making in MANET are for the most part focused on utilizing reliability or cost based components to accomplish the coveted impact of hubs participation. [6][7]

Misbehaviour in its more awful frame includes a consider expectation by a hub or gathering of hubs disturb the activity of the system for its destinations, such hubs are named malicious and managing them would include the arrears of giving security in MANETs.

Notwithstanding the vast majority of the outstanding assaults and dangers that the wires and remote system endured, MANETs are likewise subject to an expansive number of extra assaults and dangers, the different open security issues for MANETs are, yet not restricted to:

1. Misbehaviour location
2. Key dispersion and administration
3. Denial of Services techniques
4. Security engineering
5. Vulnerability investigation of different existing MANET organize protocols

III. Malicious Hubs in MAnet

These hubs expect to get the best advantages from the systems while attempting to safeguard their own particular assets, e.g. battery life or transmission capacity. Malicious hubs endeavor to keep up interchanges with the hubs it need to send information packets to however may decline to co-work when it gets steering or information packets that it has no enthusiasm for. In this way, it might either drop information packets or decline to retransmit directing packets that it has no enthusiasm for. [7][8]

The malicious hub can do the accompanying conceivable activities in specially appointed system:

1. Turn off its Power when it doesn't have dynamic correspondences with different hubs.
2. Does not rebroadcast Route ask for (PREQ) when it gets a RREQ.
3. Rebroadcasts RREQ yet does not forward Route answer (RREP) on turn around course, accordingly the source does not know a course to the goal and it needs to rebroadcast a RREQ.
4. Rebroadcasts RREQ, forward RREP on turn around course however does not forward information packets.
5. Will not unicast communicate Route mistake (RERR) packets when information packets are gotten however there is no course.
6. Selectively drop information packets.

This specific can be utilized to battle existing instruments to distinguish malicious hubs. In light of the above dangers we can perceive how harming malicious hubs can be MANET, especially regarding decreasing the conveyance rate by dropping packets and bot sending them which prompt wastefully in MANET. Enhancing the proportion of very much carried on hubs thusly brings about better trust among hubs, better security, and henceforth better general task of the MANET.[8-12]

IV. AODV Routing Protocol Architecture

AODV Routing Protocol consists of the following main objective:

1. To communicate the disclosure parcels just when it is Mandatory.
2. To recognize B/w nearby availability (neighborhood) and general topology support.
3. To pass information that involves the adjustments in neighborhood availability for those adjacent versatile hubs which are likely need this information.

Route Discovery Process:

Source in the system will start course disclosure by communicating a RREQ to the close-by hubs in the network. RREQ comprises of the accompanying fields: source_address, source_sequence, broadcast_id, dest_address, dest_sequence, hop_count. On the off chance that any hub doesn't satisfy the RREQ condition, it will break the information to establish the reverse path setup or forward way setup will go with the transmission of RREQ.

1. Destination IP addresses.
2. Source IP address.
3. Broadcast_IP.
4. Source node’s sequence number.
5. Expiration time.

Forward path setup:

In the forward way setup the RREP ventures shape the goal D to the source hub 5 hub that are not has a place with the way decided/recognized by the RREP will timeout after ACTIVE_ROUTE_TIMEOUT(3000ms) and will wreck the turnaround pointers.

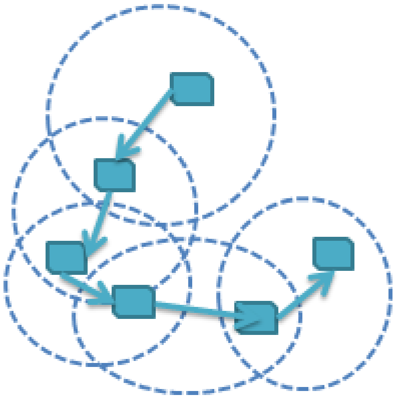


Figure 2: Forward Path Setup

Reverse path setup:
To develop a turnaround way, hub store the address of the neighbor from which it gather the principal duplicate of RREQ. These Reverse way course sections are kept up for at any rate enough time for the RREQ to navigate a N/W or give a reaction to the sender. Figure 3 represents the reverse path setup

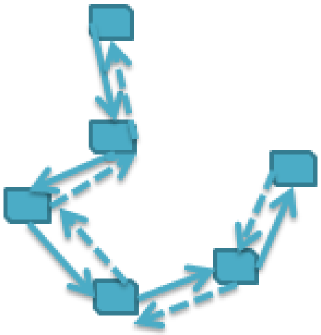


Figure 3: Reverse Path Setup

Route Table Management:-

The Route table Management not just contains the source and goal arrangement no., yet additionally contain the course table passages, which is called delicate state related with the section. Our critical angle with directing sections is the course reserving time out or the time after which the course is thought to be invalid. Each Route table passage contains the information:-

- Target
- Next Prance
- Numbers of hop
- Sequence number for the destination
- Active neighbor for this route
- Expiration time for the route table entry

Path Maintenance

The development of hubs not relies upon the dynamic way and doesn't influence the steering to that way goal. At whatever point a transmitting hub moves with a dynamic session, transmitting hub can start course revelation procedure to identify crisp way to the goal. Connection disappointment is likewise show if endeavour's to advances Packets to the following bounce fall flat. Once the following jump winds up inaccessible, the centre point upstream of the break causes an unconstrained RREP with another progression number and ricochet count of unlimited quality to all unique upstream neighbours.

V. New Secure Framework – MANET Communication

New technique is based on the seven steps control mechanism to detect, isolate and prevent data from malicious node in the network communication process. For the base any routing protocol can be used that support multipath routing such as AODC for multipath routing. Figure 4 represents the flow diagram of the routing algorithm after implementing secure control mechanism.

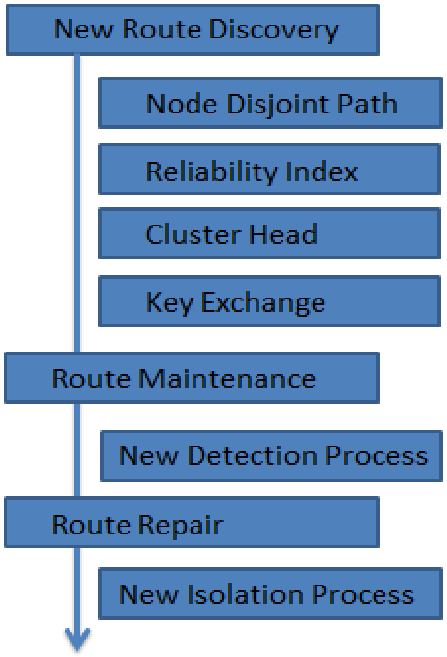


Figure 4 New Security Algorithms for MANET

Data Prevention using Distribution technique

In the third step we will prevent the packet data in the network by using network knowledge that we have gathered during step 1 & step 2. In this step we will use dispersion technique, for this packet packets will be forwarded by the all possible route from the disjoint node multiple path sets and all packets are reassembles by the destination nodes when received. However if any packet is lost in the communication process that lost packet will have negligible effect on assembling data at source. Figure 7 represents the distribution technique.

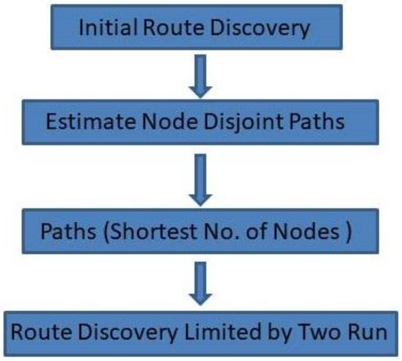

Initial Route Discovery
Estimate Node Disjoint Paths
Paths (Shortest No. of Nodes)
Route Discovery Limited by Two Run

Figure 5: Estimation of Multiple Path Sets

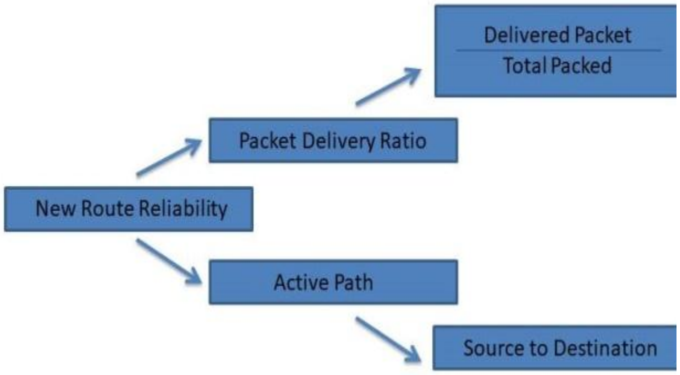


Figure 6: New Reliability Index

Control Packet

In this two new packets are defined that will help in the communication process for detection & prevention of malicious nodes in the network. First packet will be used by source while sending data packets to the destination. And second packet is used by destination to provide information about data packet received by it. This added communication will helps in detection and isolation of malicious nodes in the network. First packet is "PI" stands for PACKET INFORMATION that consists of following information Data age rate, Data parcel measure, Data Amount, Path Information, Path length, and hubs along way. Figure 8 represents the PI packet.

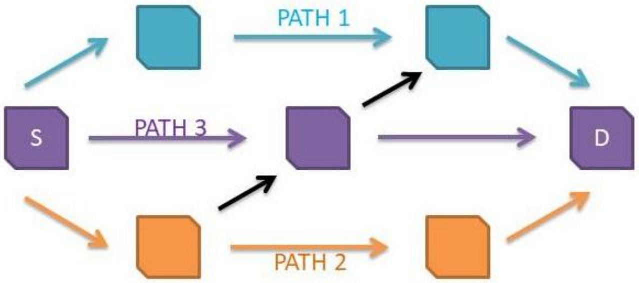


Figure 7 Data Prevention Using Distribution Techniques

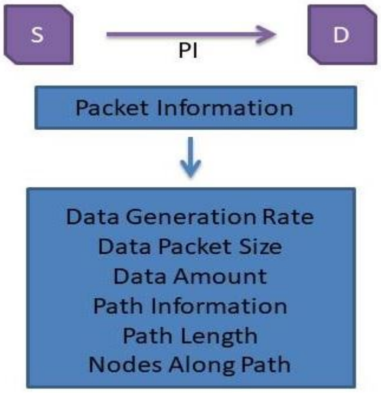


Figure 8 PI Packet Representations

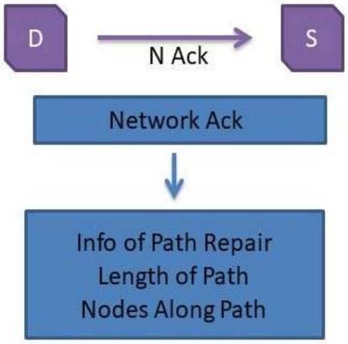


Figure 9 N ACK Representations

Second packet is "N ACK" stands for Network Acknowledgement Packet that consists of Information regarding path repair, Length of Path, Nodes along path from which data packet is received. Figure 9 represents the N ACK Packet.

Packet Authentication Mechanism

In this the fifth step in secure commination process. In this process network cluster head will be used for key exchange mechanism. Key exchange mechanism will be exactly same that are used in industry from exchange public & privet key for authentication process. Figure 10 represent the Key Exchange using Cluster Head in the network.

Detection of Malicious Nodes

This is the step where malicious nodes are detected in the network. All the detection process is performed at the destination node in the network. For the detection process destination will maintain two new routing tables. One of them is temporary routing table that will be used at the start of communication link with source, second is permanent table that will be kept till the communication process ends between source and the destination. Figure 11 contains the structure of both routing table at destination node. Both of these tables are named as PATH TABLES.

Detection Mechanism

Whenever destination node in the network receives the PI packet from source which is willing to communicate with it then destination will add new path table regarding that particular source that is willing to communicate with it. Now destination will compare packet PI data with the actual data in communication. If data of PI packet is same with actual packet data received than destination move the route data to the confirmed path table.

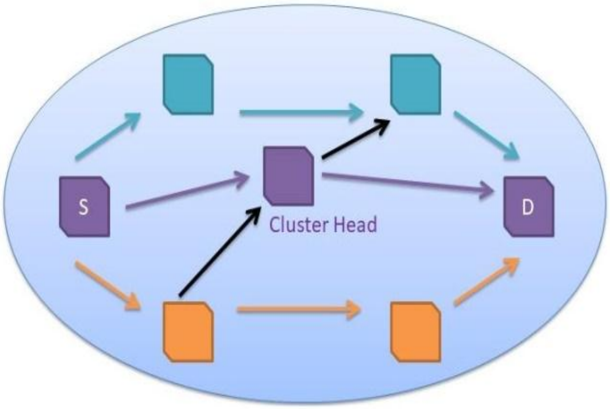


Figure 10 Key Exchange using Cluster Head

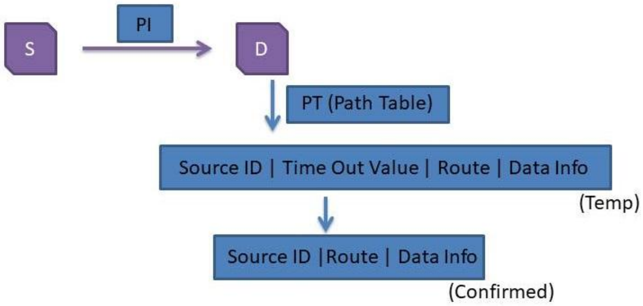

S
PI
D
PT (Path Table)
Source ID | Time Out Value | Route | Data Info
(Temp)
Source ID |Route | Data Info
(Confirmed)

Figure 11 Routing table at Destination Node

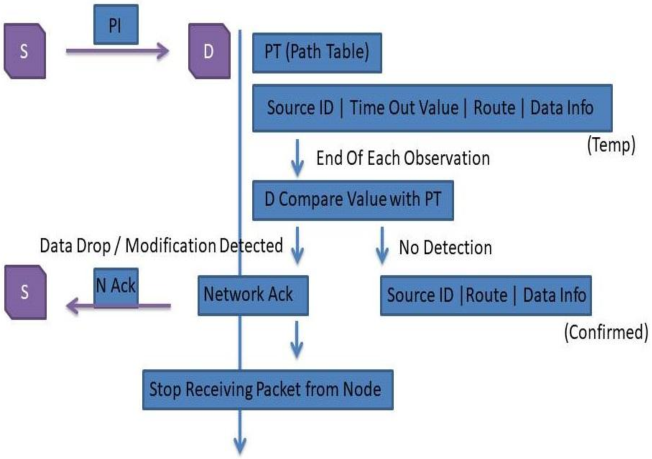

S
PI
D
PT (Path Table)
Source ID | Time Out Value | Route | Data Info
(Temp)
End Of Each Observation
D Compare Value with PT
Data Drop / Modification Detected
No Detection
S
N Ack
Network Ack
Source ID |Route | Data Info
(Confirmed)
Stop Receiving Packet from Node

Figure 12 Detection Mechanisms at Destination

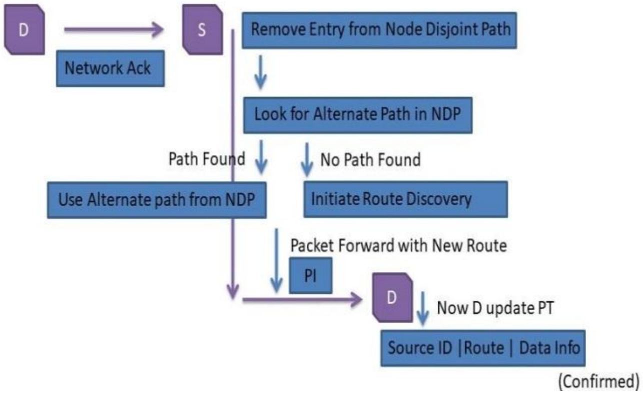

D
S
Remove Entry from Node Disjoint Path
Network Ack
Look for Alternate Path in NDP
Path Found
No Path Found
Use Alternate path from NDP
Initiate Route Discovery
Packet Forward with New Route
PI
D
Now D update PT
Source ID |Route | Data Info
(Confirmed)

Figure 13 Isolation Mechanisms at Source

Else generate “N ACK” packet with information regarding network errors that will include data regarding malicious node that tempered the route or data of the actual packet in between communication process. If “N ACK” packet is generated then destination will drop the entire data packet received through that route from the source. Figure 12 represents the complete detection mechanism of malicious nodes at the destination node in the network.

Isolation of Malicious Nodes

This will be the last step toward secure control mechanism. In this whenever any source receives” N ACK” packet from its destination than source at that time remove that particular path from its disjoint multiple path sets and communication will takes place with rest of available route in the disjoint multiple path sets based on the reliability index of paths.

This removal path from disjoint multiple path sets and isolate the malicious nodes from the communication process. Note that we can avoid communication through the malicious node in the network by isolation it from the communication process and we can’t physical remove malicious node from the network this is due to nature of network as every node is independent of each other. Now if no alternate route is available in the disjoint multiple path sets than source node will initiate route discovery process as per protocol set rules. Figure 13 represents the isolation mechanism at source node in the network.

VI. SIMULATOR SETUP & RESULTS

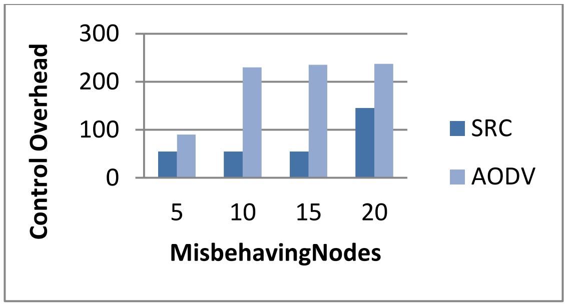
Simulator Setup

New secure structure, named it as "Secure Routing Communication". Network Simulator 3 on UBUNTU Linux stage is utilized to execute the new secure structure. Network simulator has been run no of time by varying no. of parameters. For one case parameters are defined below. Case one, the channel limit of portable hosts is set for 2 Mbps; and will utilizes the appropriated coordination capacity of IEEE 802.11 for remote LANs as the MAC layer tradition. As it has the value to educate the framework layer about association breakage. In this generation, 50 adaptable center points move in a 120 m × 120 m region for 200 seconds amusement time. We take that each center point are self-sufficiently with a typical speed. All center points have a comparable transmission extent of 70 meters. In this versatility demonstrate, a hub arbitrarily chooses a goal hub in the system. Hubs in the system are allowed to moves haphazardly toward any path with negligible of speed 5 m/s and maximal speed of 10 m/s. the reproduced action is reliable Bit Rate (CBR). We move the no. of getting unruly center points as 5, 10, 15 and 20.

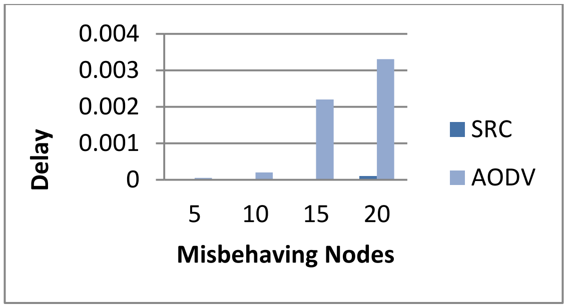
Performance Metrics

For assessment and contrast of SRC and existing AODV execution following strategies is embraced:

1. Control Overhead: The control overhead is portrayed as the aggregate number of control pallet institutionalized by the aggregate number of got data bundles. Graph 1 addresses the Control overhead outcome.
2. Normal End to-to-End Delay: The conclusion to-end postpone is discovered the center estimation of over each surviving datum parcels from the sources to the objectives. Graph 2 addresses the typical end to end delay.
3. Normal parcel conveyance extent: It is the extent of the amount of bundles got adequately to the total number of bundles sent. Graph 3 addresses the parcel conveyance extent.

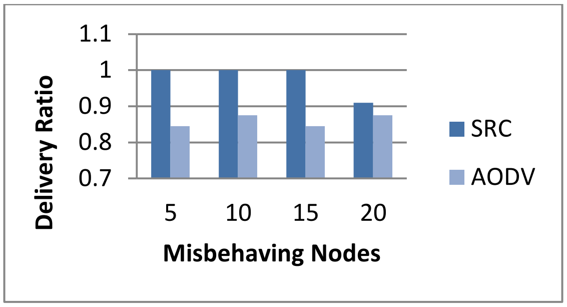


Graph 1: Control Overhead



Graph 2: End to End Delay

This security system includes: Detection of malignant hubs by the goal hub, seclusion of noxious hubs by disposing of the way and counteractive action information parcels by utilizing scattering methods. This SRC comprises of another multipath steering calculation, which decides an arrangement of hub disjoint ways. The ways are orchestrated in the plummeting and transmitted at the same time through the solid disjoint ways. The information divide the transmission is sent through the fundamental tried and true way. At the objective, if there is screw up between the transmission information and the data bundles recovered, a negative feedback is sent to the source which contains the purposes of enthusiasm of the affected ways. The source right now discards the impacted path from the summary of centre point disjoint ways.



Graph 3: packet Delivery Ration

Since the data groups are scattered along different ways using a great disseminating estimation, the goal can recoup the information effectively, there by accomplishing unwavering quality. This reproduction comes about demonstrate that, when contrasted and leaving plan, this structure decreases overhead and deferral, in the meantime it increments up parcel conveyance proportion.

VII. Conclusion and Future Scope

Routing in any system is most prone to attacks in ADHOC networks. This drawback can introduce no. of vulnerability risk in network nodes, or even the whole network. For solution to this, new framework is represented for secure communication that consists of disjoint node multiple path sets, which determines set of disjoint paths. Further reliability index for every path is calculated and are arranged in decreasing manner, so that top most path is most reliable. Further distribution technique is used for data transmission along with detection of malicious node at the destination node under route maintenance phase and isolation process at source under route repair phase in any multi path routing protocol. This new framework will decrease the delay and network overhead with increases in packet delivery ration by preventing the network from malicious nodes.

With new defined secure communication process further opportunity are also present to encounter malicious nodes in the MANET as attacks always in hunt of new process to attack on the network.

REFERENCES

[1] Al-Shurman, M., Yoo, S. M., & Park, S. "Black hole attack in mobile ad hoc networks" , In ACM-SE 42 Proceedings of the 42nd annual Southeast regional conference. 2014

[2] Balachandran, R. K., Ramamurthy, B., Zou, X., &Vinodchandran, N, "An efficient key agreement scheme for secure group communications in wireless ad hoc networks" In IEEE ICC. 2005

[3] Capkun, S., Buttyan, L., & Hubaux, J. P. ,"Sector: Secure tracking of node encounters in multi-hop wireless networks." In ACM workshop on security of ad hoc and sensor networks. 2003

[4] Cordasco, J., & Wetzel, S., "Cryptographic vs. trust-based methods for manet routing security". Electronic Notes in Theoretical Computer Science, 197(2). 2008

[5] Dabideen, S., & Garcia-Luna-Aceves, J.,"Ordering in time: A new routing approach for wireless networks." In Proceedings of IEEE MASS. 2010

[6] Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS'02), ACM, November 2002.

[7] K. Lu, Y. Qian, M. Guizani, and H.-H. Chen, "A framework for a distributed key management scheme in heterogeneous wireless sensor networks," IEEE Transactions on Wireless Communications, vol. 7, no. 2, 2008.

[8] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in Proceedings of the IEEE Symposium on Security And Privacy, May 2003.

[9] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," ACM Transactions on Information and System Security, vol. 8, no. 2, 2005.

[10] D. Liu, P. Ning, and L. I. Rongfang, "Establishing pairwise keys in distributed sensor networks," ACM Transactions on Information and System Security, vol. 8, no. 1, 2005.

[11] Khatri P, Rajput M, Shastri A, Solanki K, "Performance study of ad-hoc reactive routing protocols" J ComputSci 6(10):1159–1163, 2010

[12] Medadian M, Yektaie MH, Rahmani AM,"Combat with black hole attack in AODV routing protocol in MANET". In: First asianhimalayas international conference on internet, IEEE Press, New York, 2009

[13] Gwertzman, J.S. and M. Seltzer. "The Case for Geographical Push-Caching" Workshop on Hot Operating Systems. 1995.

[14] Kleinrock, L., "Nomadic Computing (Keynote Address)." In Int. Conf. on Mobile Computing and Networking., Berkeley, CA. 1995

[15] Amir, E., S. McCanne, and H. Zhang. A n Application Level Video Gateway. inA C M Multimedia '95. 1995. San Francisco, CA.

[16] Le, M.T., F. Burghardt, and J. Rabaey, "Software Architecture of the Infopad System." In Mobidata Workshop on Mobile and Wireless Information Systems, New Brunswick, NJ. 1994

[17] Pasquale, J.C., et al., "Filter Propagation in Dissemination Trees: Trading Off Bandwidth and Processing in Continuous Media Networks." In 4th Intl. Workshop on Network and Operating System Support for Digital Audio and Video. 1993.

[18] Clark, D.D. "The Design Philosophy of the DARPA Internet Protocls". In ACM Sigcomm Symposium. Stanford, CA. 1988

[19] Von Eicken, T., et al."Active Messages: A Mechanism for Integrated Communication and Computation". In 19th Int. Symp. on Computer Architecture. Gold Coast, Australia. 1992

[20] Agarwal, A., et al., "The MIT Alewife Machine: Architecture and Performance". In 22nd Int. Symp. On Computer Architecture (ISCA '95). 1995.

[21] O'Malley, S.W. and L.L. Peterson, "A Dynamic Network Architecture". ACM Transactions on Computer Systems, 10(2) p. 110-143. 1992

[22] Jones, M. "Interposition Agents: Transparently Interposing User Code at the System Interface". In 14th ACM Symp. On Operating Systems Principles. Asheville, NC. 1993

[23] Bershad, B., et al. Extensibility, Safety and Performance in the SPIN Operating System. In 15th ACM Symp. On Operating Systems Principles. 1995.

[24] Engler, D.R., M.F. Kaashoek, and J. O'Toole Jr. Exokernel, Operating System Architecture for Application-Level Resource Management". In 15th ACM Symp. on Operating Systems Principles. 1995.

[25] Borenstein, N. "Email with a Mind of its Own: The Safe-Tcl Language for Enabled Mail." In IFIP International Conference. Barcelona, Spain. 1994

[26] Gosling, J. and H. McGilton, "The Java Language Environment: A White Paper", Sun Microsystems. 1995

[27] Gosling, J. "Java Intermediate Bytecodes", In SIGPLAN Workshop on Intermediate Representations (IR95). San Francisco, CA. 1995