Multipath Distance Vector Routing using Intrusion detection system in MANET

M.P Mahadeva Prasad[1], Vani Ashok[2]
[1]*M.Tech 2nd Year, Department of computer Science and Engineering, JSS Science and technology University, Mysuru, Karnataka, India*
[2] *Assistant Professor, Department of Computer Science & Engineering, JSS Science and technology University, Mysuru, Karnataka, India*

Abstract- **A mobile ad hoc network (MANET) is a collection of wireless nodes, which works well only if those mobile nodes are good and behave cooperatively. The lack of infrastructure support and resource constraint is the key issue that causes dishonest and non-co-operative nodes. Therefore, MANET is vulnerable to serious attacks. To reduce the hazards from such nodes and enhance the security of the network, this work supports an Ad hoc On-Demand Multipath Distance Vector (AOMDV) Routing protocol, named as Trust-based Secured Ad hoc On-demand Multipath Distance Vector (TS-AOMDV), which is based on the nodes' routing behaviour. The proposed TS-AOMDV aims at identifying and isolating the attacks such as flooding, black hole, and gray hole attacks in MANET. With the help of Intrusion Detection System (IDS) and trust-based routing, attack identification and isolation are carried out in two phases of routing such as route discovery and data forwarding phase. IDS facilitates complete routing security by observing both control packets and data packets that are involved in the route identification and the data forwarding phases. To improve the routing performance, the IDS integrates the measured statistics into the AOMDV routing protocol for the detection of attackers. This facilitates the TS-AOMDV to provide better routing performance and security in MANET. Finally, the Trust-based Secured AOMDV gives more security than the existing AOMDV.**

Index Terms- **Mobile Ad-hoc Network, Intution Detection System, Attack Identification and isolation, Multiaath Routing.**

I. INTRODUCTION

An adaptable uniquely delegated framework (MANET) is a social event of remote centres, which works splendidly just if those convenient centres are extraordinary and bear on pleasantly. The nonappearance of structure support and resource impediment is the key issue that causes deceitful and non-co-operator centres. Along these lines, MANET is vulnerable against honest to goodness strikes. To reduce the dangers from such focuses and upgrade the security of the system, this paper grows an Ad hoc On-Demand Multipath Distance Vector (AOMDV) Routing custom, named as Trust-create Secured Ad hoc concerning request Multipath Distance Vector (TS-AOMDV), which depends upon the focuses' coordinating conduct.

The recent trends in wireless communications have changed the lives of the human beings. The new wireless technologies create a tremendous potential for the next generation Mobile Ad-hoc Networks (MANETs) and applications. The arrival of wireless technologies such as Bluetooth and Wi-Fi increases the scope of the ad hoc networking and enables potential applications in the personal and local area networking scenarios. Due to the ubiquitous handling, it is a challenging task to attain proficient wireless intercommunication over mobile devices. The MANET is a multi-hop distributed communication network comprising of a collection of mobile nodes that operate in a dynamic and self organized manner. The network connectivity changes dynamically due to the random mobility of mobile nodes in the absence of access point or any predefined infrastructure. Each mobile node performs the data forwarding only through single or multi-hop communication due to the limited transmission range. The design of routing protocols is used to find a suitable path to route the data packet from the source to the destination. The routing process has to evolve efficiently and enhance the efficiency of the routing

process in the presence of dynamic network conditions, unpredictable mobility, limited energy, autonomous architecture, and resource constrained environment. The short communication range and lack of infrastructure are the major reasons for collaborative communication model. In a MANET, the mobile node forming dynamic network topology and the nodes located within the transmission range of a node are called neighbours. The neighbours transmit the data packets directly to the other nodes within the communications range. However, a node transmits the data through a sequence of multiple hops, with intermediate nodes, when it wants to send the data packet to a non neighbouring node or a distant node. The diversity of potential applications in the MANET promotes a broad range of routing protocols to fulfil the requirements. The major focus of the routing is the performance and the efficiency of the protocol in the presence of a dynamic network environment. The routing protocol has to overcome the security pitfalls to utilize the potentials of the MANET. A secure routing is challenging due to the security vulnerabilities present in the network.

II. RELATED WORK

Routing protocols in mobile ad hoc and sensor networks discover usable multi-hop routes between source and destination nodes. However, some of the routes found and used may not be as reliable or trustable as expected. Thus, finding a trusted route is an important component for enhancing the security of communication. They present a trust-based routing protocol for enhanced security of communication in mobile ad hoc networks (MANETs) and wireless sensor networks (WSNs). Enhanced trust and security are achieved by the maintenance of a trust factor by the nodes in the network. This factor is established and refined over time and it increases for each node when it participates successfully in data transmissions. Simulation experiments are performed to verify the operation of the proposed protocol and evaluate its performance. For the protection of both routing and data forwarding operations, a network layer security solution has been provided as a solution for various security attacks in ad hoc networks. In this paper, to develop a security framework had proposed by authors. Security framework involves: Detection of malicious nodes by the destination node, isolation of malicious nodes by discarding the path and prevention data packets by using dispersion techniques. They propose to develop a Multipath Reliable Routing (MRR) algorithm, which determines a set of node-disjoint reliable paths. The paths are arranged in the descending order of their reliability index. Data packets are dispersed and transmitted simultaneously through the reliable disjoint paths. The primary reliable path sends the information packet containing the transmission information. At the destination, if there is mismatch between the transmission information and the data packets received, a negative feedback is sent back to the source that includes the particulars of the affected paths. The affected paths are then removed from the list of node-disjoint paths by the source. The destination can recover the data effectively by attaining reliability, the data packets are dispersed along multiple paths using an efficient dispersion algorithm. Their simulation result shows that, when compared with existing scheme, their framework reduces overhead and delay, at same time increasing the packet delivery ratio.

MANET routing protocols are designed based on the assumption that all nodes cooperate without maliciously disrupting the operation of the routing protocol. AODV is a reactive MANET routing protocol that is vulnerable to a dramatic collapse of network performance in the presence of black hole attack. This work shows a new concept of Self-Protocol Trustiness (SPT) in which detecting a malicious intruder is accomplished by complying with the normal protocol behaviour and lures the malicious node to give an implicit avowal of its malicious behaviour. They present a Blackhole Resisting Mechanism (BRM) to resist such attacks that can be incorporated into any reactive routing protocol. It does not require expensive cryptography or authentication mechanisms, but relies on locally applied timers and thresholds to classify nodes as malicious. No modifications to the packet formats are needed, so the overhead is a small amount of calculation at nodes, and no extra communication. Using NS2 simulation, they compare the performance of networks using AODV under blackhole attacks with and without our mechanism to SAODV, showing that it significantly reduces the effect of a blackhole attack.

III PROBLEM STATEMENT

The MANET needs to provide a reliable and secure routing over mission-critical environments like healthcare and military applications. Several routing techniques have been proposed in the mobile ad-hoc networks. These protocols work well in benign environments, where the mobile nodes are highly trusted. Therefore, it is necessary to modify these protocols substantially if they are used in a hostile network environment. The MANET maximizes throughput by using all available nodes for routing and forwarding. Stimulating cooperation among the nodes in the network is the one of the key issues in MANETs. It makes use of all nodes in the network for broadcasting and routing if nodes are co-operative and well behaving. The major challenge in designing such a self organized network is the detection of the routing attacks. The steady increase of attacking nodes will severely degrade the routing performance. The attacking nodes must be detected and eliminated effectively to improve the performance of the network. Another important problem of wireless communication over infrastructure-less networks is the unpredictable node mobility. The node mobility leads to frequent link failures in single path routing, resulting in poor network throughput. Thus, to balance the network throughput and reliable data delivery, it is essential to incorporate multipath routing and an efficient trust evaluation model in hostile environments. The security issues in multipath routing are not considered in the conventional routing techniques. In other words, the existing multipath routing protocols are not designed with the aim of provisioning security in mind. The most important factors to include in the security provision are the availability, reliability, resiliency, and self-healing.

IV System Architecture

In TS-AOMDV, the IDS runs on each node, and it monitors the neighbouring nodes' routing activities at the network layer to detect the routing attackers. It performs continuous data monitoring to identify the behaviour of the nodes and to measure the routing packet generation rate and determine data forwarding statistics. An IDS facilitates a complete routing security by observing both the control packets and data packets that involve in the route identification and the data forwarding phases. The measured statistics are integrated into the AOMDV routing protocol for the detection of attackers. To improve the routing performance, the IDS convert the measured statistics into trust values that are used in the route discovery and data forwarding phases of TS-AOMDV. It facilitates the TS-AOMDV to provide better routing performance and security in MANET. The architecture of TS-AOMDV

An adaptable uniquely delegated framework (MANET) is a social event of remote centers, which works splendidly just if those convenient centers are extraordinary and bear on pleasantly. The nonappearance of structure support and resource impediment is the key issue that causes deceitful and non-co-operator centers. Along these lines, MANET is vulnerable against honest to goodness strikes. To reduce the dangers from such focuses and upgrade the security of the system, this paper grows an Ad hoc On-Demand Multipath Distance Vector (AOMDV) Routing custom, named as Trust-create Secured Ad hoc concerning request Multipath Distance Vector (TS-AOMDV), which depends upon the focuses' coordinating conduct.

The proposed TS-AOMDV aims to identify and isolate the attacks such as flooding, black hole, and a gray hole in a MANET. With the aid of an IDS and a trust-based routing, the attack identification and isolation are carried out in two phases of routing such as route discovery phase and data forwarding phase. In the route discovery phase, an attacker launches the route request flooding attack, in which it floods the routing packet with the nonexistent destination address in the network. An IDS monitors the packet generation rate of the source and assigns an inversely proportional value of the request packet count as the 'source-trust value' of the corresponding source. When the trust value of the source reaches the threshold, the route request packet from the attacker source is dropped. In data forwarding phase, an attacker that involves as a router drops the packet instead of forwarding. The IDS monitors the packet forwarding activity of the router and assigns the 'route trust value' as the ratio between the forwarded packet count and the received packet count. When the trust value of the router reaches the threshold, it selects an alternate path from the multiple available paths that are stored in the routing table and resumes the data transmission through it.

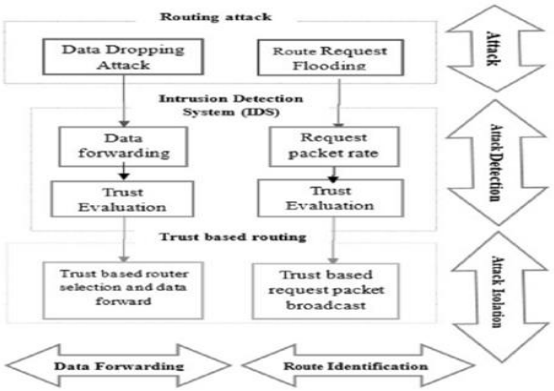

Fig 1:TS-AOMDV Architecture

1. Route Identification Phase

With the help of IDS and trust-based routing, the attack identification and isolation in TS-AOMDV are carried out in two phases of routing such as route discovery phase and data forwarding phase. The trust obtained from IDS is applied in the routing decision-making about propagating RREQ packet of the source and selecting the trust based router for data forwarding. Initially, each node assigns the trust value as 'one' to its neighbouring nodes. According to the routing activities of these nodes, the IDS measures the original trust value and informs the network layer. The route discovery process is carried out based on the trust value to isolate the flooding attacker activity. Prior to rebroadcasting the received RREQ packet to the neighbours, every node checks for the trust value of the source that has broadcasted the RREQ packet.

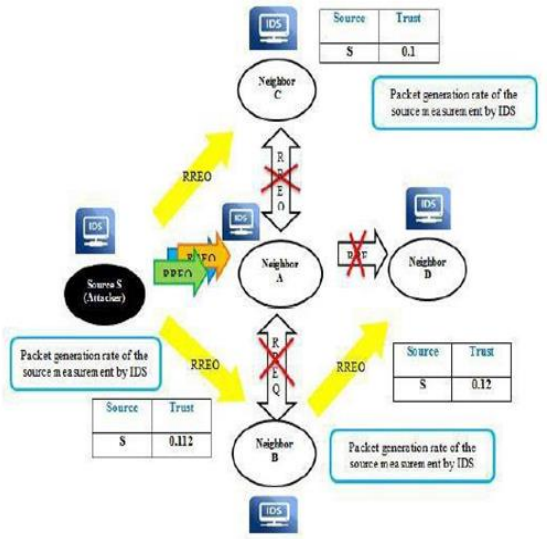

Fig 2: Route Identification Phase

2. Data forwarding phase

Data forwarding process is carried out based on the trust value to isolate the activity of black hole and the gray hole attacker. Prior to forwarding the data packet to the router, every node checks for the trust value of the router. The trust value of the router indicates the reliability of data delivery through it. If the trust value is low, the current data transmission through the malicious router is blocked. Subsequently, the trusted router from the routing table is accessed to resume data transmission through it. For instance, in figure 3 the trust value of the node B is higher than node A, and so the source node selects router B for further data forwarding. Thus, the IDS and the trust based TS-AOMDV protocol improves the routing performance and security in MANET.

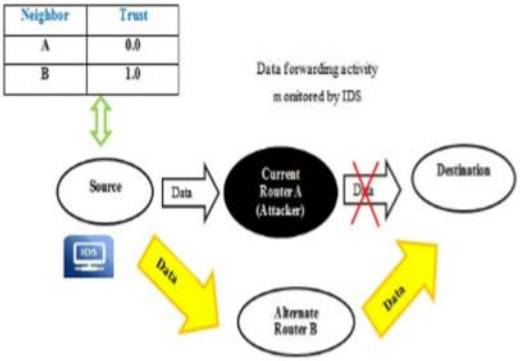

Fig 2: Data Forwarding Phase

V RESULTS

Results obtained after implementation of the modules and discussions from various standpoints are presented and assessed in this chapter. All the conclusion and inferences are based on the qualitative aspects of the project and aim to cover the significance and impact of the Automated Engine to Manage Machine Data Agents as there is little scope for quantitative analysis for the proposed enhancements. This section explains the results of this project and also the final outcome of the below modules implemented in this project.

1. One Hop Neighbour Identification Module

Each hub distinguishes its one jump neighbours utilizing HELLO Exchange (UDP) And Each identified one hop neighbors are set with 2

variables/parameters i.e “Source- Trust” & “Router-Trust” and initialized to its default values i.e “1”

2. Route Discovery Module

DSR (AODV) Routing Protocol to find an optimal path between any source and destination nodes And Avoid accepting RREP packets from those nodes whose Source-Trust & Router- Trust parameter are abnormal. Hence selects only optimal & secure path between any give source and destination node And Compute Backup paths at each node for respective destination (Computed during RREPs received at each node)

3. Flooding Attack Detection Module

IDS service is deployed at each node to monitor the every neighbouring nodes And In case of RREQ packet reception, IDS extracts Ip Address of the packet originating node and increments the RREQ count of the corresponding source (Reset the counter based on some timer - Enhancement) And Source-Trust Parameter is figured by, Source-Trust = (RREQ Count)- 1 And In the event that the Source-Trust Parameter esteem is lesser than the limit, at that point the RREQ bundle from the relating source is dropped (rather than rebroadcasting) to obstruct the flooding action of the assailant

4. Data Transmission Module

Uses Multi hop Data Transmission Protocol (TCP) , Uses End 2 End Acknowledgement Scheme, Uses time-out timer named ACK_REC_TOT (Acknowledgment Reception Time- Out-Timer) for Acknowledgement Reception

5. Black & Gray Hole Attack Detection Module

IDS service is deployed at each node to monitor the neighbouring node that is selected for data transmission And IDS benefit processes Router-Trust Parameter of chose neighbouring hub utilizing, Router-Trust = Received Packet Count/Forwarded Packet Count And If the Router-Trust Parameter esteem is lesser than the edge, the present information transmission through the pernicious switch is blocked. Along these lines, the put stock in switch (Backup Path) from the steering table is gotten to continue information transmission

VI CONCLUSION

a Trust-construct Secured Ad hoc With respect to request Multipath Distance Vector, TS-AOMDV was unmistakably intended to accomplish security in MANET. The proposed convention is versatile and confrontational with two kinds of steering assaults propelled over information bundles and control parcels, for example, dark gap and dark opening, and demand parcel flooding assault. The IDS connected with every hub, performs two tasks, for example, estimating the course ask for age rate of the source, and bundle sending insights of the neighbours amid the course revelation and information sending stage separately.

By contrasting these qualities and the edge, the IDS effectively catches the diverse kinds of aggressors in different steering stages. The deliberate measurements are fused into trust esteems for choosing the most trusted way to enhance the execution of TS-AOMDV. In addition, the execution of the proposed convention is reproduced utilizing NS2. The proposed Trust based Secured AOMDV (TS-AOMDV) is contrasted and the current AOMDV as far as throughput, course determination time, trust non-use factor, vitality utilization and overhead through the recreation show. The reproduced comes about demonstrate the prevalence of the proposed convention in different situations.

REFERENCES

[1] Erciyes, K. "Distributed Graph Algorithms for Computer Networks", Compute Communications and Networks , London: Springer, pp. 259- 275, 2013.

[2] S. Abdel Hamid, H. Hassanein and G. Takahara, "Routing for Wireless Multi-Hop Networks: Unifying Features", SpringerBriefs in Computer Science, pp. 11-23, 2013.

[3] Hamid, S. A., Hassanein, H., & Takahara, G., “Routing for Wireless Multi Hop Networks– Unifying and Distinguishing Features”, School of Comp.—Queen’s University, Canada, report 583, 2011.

[4] Habib, S., Saleem, S., & Saqib, K. M., “Review on MANET routing protocols and challenges”, IEEE Student Conference on Research and Development SCOReD , pp. 529-533 , 2013.

[5] A. Ahmed, K. Abu Bakar, M. Channa, K. Haseeb and A. Khan, "A survey on trust based detection and isolation of malicious nodes in adhoc and sensor networks", Frontiers of Computer Science, vol. 9, no. 2, pp. 280-296, 2015.

[6] I. Abdel-Halim, H. Fahmy and A. Bahaa-Eldin, "Agent-based trusted on-demand routing protocol for mobile ad-hoc networks", Wireless Netw, vol. 21, no. 2, pp. 467-483, 2015.

[7] Mahmoud, Mohamed MEA, and Xuemin Sherman Shen. "Secure routing protocols." Security for Multi-hop Wireless Networks. Springer International Publishing, pp. 63-93, 2014.

[8] Shanmuganathan, V., and T. Anand. "A Survey on Gray Hole Attack in MANET." IRACST– International Journal of Computer Networks and Wireless Communications (IJCNWC), pp. 2250-3501, 2012.

[9] Tayal, S., & Gupta, V., "A Survey of Attacks on Manet Routing Protocols", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 2, No.6, pp. 2280-2285, 2013.

[10] Vaidya, Binod, et al. "Secure multipath routing scheme for mobile ad hoc network." Third IEEE International Symposium on Dependable, Autonomic and Secure Computing, pp. 163- 171, 2007