Modelling, Measurement and Control A
Vol. 91, No. 2, June, 2018, pp. 73-76
Journal homepage:http://iieta.org/Journals/MMC/MMC_A

Effective multi-mode routing mechanism with master-slave technique and reduction of packet droppings using 2-ACK scheme in MANETS

Vejendla L. Narayana*, Chettiar R. Bharathi

Department of CSE, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamil Nadu. & Asst. Prof., Vignan's Nirula Institute of Technology & Science for Women, Guntur, Andhra Pradesh 522005, India

Corresponding Author Email: lakshmanv58@gmail.com

Received: June 11 2018
Accepted: June 30 2018

Keywords:
Mobile Ad hoc Network (MANET), routing, end-to-end cryptography, I-AODV, packet drop, 2ACK approach

ABSTRACT

MANET is an accumulation of portable nodes that are equipped for imparting each other by means of a remote connection. MANET can frame at wherever necessary without any fixed infrastructure. There are sure parameters those are identified with the execution of the MANET i.e. routing, throughput, packet drop, delay and so forth. For secure data transmission cryptographic mechanisms are used and routing should be done dynamically so that nodes could easily find the shortest path for data delivery from source to destination and Private Key Generator (PKG) is used for generating keys for performing encryption and decryption of data. In this paper, we proposed a cryptographic strategy for generating the keys and for dynamic routing multi-mode routing algorithm is proposed and I-AODV protocol is also used which identifies the shortest path and allows nodes for data transfer and another strategy is proposed which mitigates the packet drop by presenting a 2ACK plan with sorting calculations.

1. INTRODUCTION

Routing is the way towards choosing paths in a network along which to send information packets. A uniquely named Routing tradition is a convention, that reins how nodes pick which route towards destination without any fixed strategy. In remarkably named systems, nodes don't begin acquainted with the topology of their structures; rather, they need to find it. Such areas and furthermore the routes operating those, nodes as next nodes are expunged [3]. By then new target comes. This is the way by which it limits.

Packet Drops occurs because of the portability, blockage, transmission failure and the assault are known as the packet drop. Henceforth,

Packet drop=sent packet –receive packet [12]

Other than these issues, MANETs experience some different significant issues like black hole, malignant assault and worm hole attack that are excessively cause packet drops. A few nodes deliberately drop the packet, these nodes are called malicious nodes. Indeed, even after the ideal determination of the route, network can't perform well because of the packet drops [5]. Nodes are in charge of packet drop in two ways [4]. nodes are disposing of the packets because of inadequate assets and nodes are disposing of the packet with no reason (malicious node).

2. RELATED WORK

There has been a considerable measure of work done on tending to packet drop in MANET. Yi Lu and Yuhui Zhong proposed a strategy to comprehend the primary issues those are specifically identified with packet drop and demonstrated that AODV has more packet drop because of the versatility as contrast with blockage; thus AODV is more delicate for portability. Shiv shakti et.al., proposed technique in which they utilized blend elements of static and in addition dynamic Routing calculation. The proposed framework is sufficiently skilled to discover the following node for conveyance of the packet. Ahead of time AODV, packet drop is less as contrast with AODV. Hemant kumar et.al, proposed a technique in which they acquainted a strategy with identified the broken connections between two nodes, route can be repaired or can be disposed of to stay away from the packet drop. The proposed strategy can keep the packet drop because of the movement thickness and stays away from the pernicious connections.

3. WORKING OF AODV

In traditional AODV, the system is tranquil until the point that a connection is required. By then the system nodes point that needs an association bestows an enthusiasm for connection. Other AODV nodes forward RREQ message, and record in the middle that they heard it from, having an effect of short lived routes back to the poor nodes point. Precisely when an inside point gets such a message and right now has a route to the coveted nodes point [10], it bestows something specific in switch through a vaporous route to the asking for nodes point.

Each adaptable host in the framework goes about as a particular switch and route are considered as required, in this way making the framework self-start [2]. Each center point in the framework keeps up a routing table [7] with the routing information sections to it's neighboring centers, and two separate counters: a center route of action number and an impart id. Right when a center (say, source center point 'S')

needs to talk with another (say, objective center 'D'), it builds its convey id and begins path divulgence by imparting a route ask distribute to its neighbors. The RREQ contains the going with fields:– originator-addr, – originator-sequence, – destination-addr, – destination-sequence, – bounce count.

3.1 Path finding process in improved-AODV

In the Proposed Method after a network is established successfully then for performing route discovery Improved-AODV method is used in which the nodes in the network has to register with the PKG. The PKG will authorize the nodes and the nodes which are successfully authorized can participate in communication. The shortest Path is calculated only between the authorized nodes.

The source node will then send the RREQ message to its authorized neighbor nodes and updates the routing table.

The Node which receives the RREQ message will forward the same request to its authorized neighbor nodes. If the route does not exist then they will send the RERR message back, otherwise they forward RREQ message to their authorized neighbors.

The process continues until destination receives RREQ message and every time the routing table gets updated. Now the destination will send the RREP message to the source and at source side routing table is updated based on Receiving the RREP message from the destination. The route which sends the RREP message early to the source will be considered as the shortest path and the route is updated in routing table.

Unlike AODV,I-AODV sends RREQ message to the authorized neighbor nodes only. Here Private Key Generator (PKG) plays a crucial role in authorization. To perform authorization the nodes energy consumption and miscellaneous behavior are considered. The nodes whose performance is good only are authorized. In AODV every time neighbor node sends RREP message back to source where as in I-AODV the destination only will send the RREP message to source. Fig-1 explains the routing method in I-AODV method. Here Green Nodes are considered as authorized nodes and the remaining are ordinary nodes.

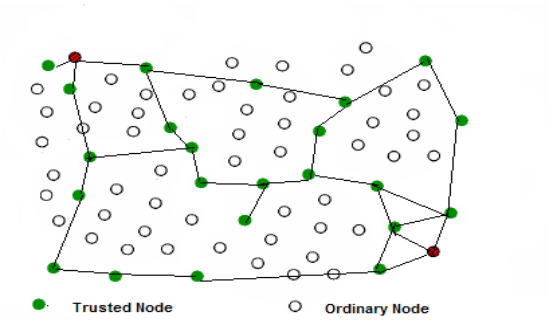

Figure 1. Routing process in I-AODV

3.2 Master-slave method

MANETs are dynamic in nature and the nodes in MANET will enter or leave the network randomly. As the PKG is also a node in the network there is chance for crash in the entire network if the PKG leaves the MANET.

To avoid such situation Master-Slave technique is used in which after selecting PKG in the network the that PKG is considered as MASTER node and it will make two authorized nodes as its slaves which are randomly chosen.

The slave nodes also maintain all the data PKG is maintaining. When a MASTER node leaves the network then immediately One of the SLAVE nodes becomes the PKG and again it makes two nodes as SLAVE nodes to it. This process continues till communication ends. By using this methodoly the failure rate of network in terms of data loss will be drastically reduced. The below figure explains the MASTER-SLAVE Method.

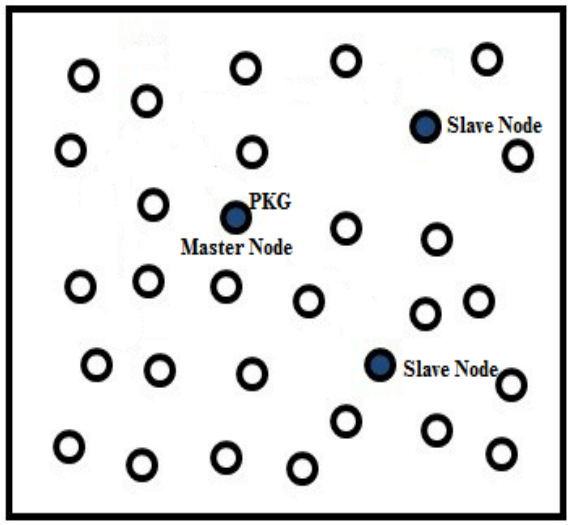

Figure 2. Master-slave method

3.3 Proposed algorithm for routing and using PKG

After successfully establishing a MANET the main problem is with the path finding and using PKG as the data at source side is encrypted with the public key and for decryption PKG issues the private key to the authorized destination. The proposed algorithm nodeses on where PKG is used and where it get relaxed. The data from the source to the destination should be reached securely in a shortest path among the MANET.

```
Algorithm Multi-Mode Routing {
if(No.of Nodes = = 2) {
Perform End to End Encryption of data among them.
}
else if(No.of Nodes = = 3) {
Consider the node other than source and destination as PKG
and perform the transmission process.
}
else if(No.of Nodes>3) {
Calculate the shortest path among the MANET and find
master and slave nodes(atleast 3 nodes) by selecting nodes
which satisfy the properties of MASTER & SLAVE nodes
and initiate the data transfer.
}
else {
End;
}  }
```

The above algorithm explains the process of data transfer method between source and destination nodes by using PKG if the MANET group has sufficient number of nodes otherwise the MANET initiates End-to-End Cryptography method for secure data transfer. After establishing path from source to destination ,in that path a node is selected as a

master node which acts as PKG. This node has 2 slaves under it as if the PKG moves out of network then a slave become master which now acts as PKG. This process continues until communication is completed.

3.3.1 End-to-end cryptography

End-to-end encryption (E2EE) is an arrangement of correspondence where just the imparting clients can read the messages. On a fundamental level, it forestalls potential spies – including telecom suppliers, Internet suppliers, and even the supplier of the correspondence benefit – from having the capacity to get to the cryptographic keys expected to unscramble the conversation.[1]The frameworks are intended to vanquish any endeavors at reconnaissance or altering in light of the fact that no outsiders can decode the information being imparted or put away. In E2EE, the data is encoded on the sender's system or contraption and simply the recipient can unravel it. Nobody amidst, be they an Internet pro association, application master center or software engineer, can read it or disturb it.The cryptographic keys used to scramble and unravel the messages are secured exclusively on the endpoints, a trap influenced possible utilizing to open key encryption.

4. PACKET DROP CAUSING LAYERS

Essentially MAC layer and system layer are in charge of all sort of packet drops[11]. MAC layer is in charge of versatility related packet drop and in addition blockage related packet drop, where as system layer is related just for portability related packet drop in routing convention.

When a packet reach system layer, routing convention is dependable to forward the packet, if a route to the destination is accessible. Packet is like to cradle until a route is accessible.

Two instances of packet drop at system layer

1. If the cushion is flood, when approaching packet should be cradled.
2. If the put away packet in support surpass the termination time (for AODV ns2 permits 30 sec time to live).

This sort of packet drop is generally happening in exceptionally powerful topology organize. CSMA/CA convention is in charge of the blockage related packet drop in MAC layer.

The reason is that

1. The back off time is high and it surpasses the point of confinement.
2. Buffer is full (space is not accessible for new approaching packet).

As MANET is exceptionally powerful in nature because of its remarkable conduct of versatility attributes; this conduct tends to connection breakage in MANET. Because of the connection breakage[11] existing route ended up noticeably inert and node find new route by route ask for packet. RREQ messages are sent by the sender when a sender node needs to impart and it is finding another route in on request steering convention, for example, AODV evidential, portability may build the quantity of route demand packet on the system.The below Table.1 illustrates the packet drop layers and the reason for such loss.

Table 1. Packet drop at MAC and network layer

	MAC layer	Network layer
Mobility related	Yes	Yes
Congestion	No	Yes

Total packet drop = (MAC layer drop) +

(Network layer drop)

5. CUSTOMIZED 2-ACK BASED METHOD

Various ACK based calculations is utilized to discover the malicious node in the system. In the current 2-ACK based plan every node sends ACK to the next hop and the received hop sends ACK to sender back. This affirmation based plan delivers a more number of ACK packets in the system. At the end of the day it expands overhead in the system and the mass measure of 2-ACK is capable to debase the system execution. Presently we changed the plan by presenting sorting calculation at the sender side. Each node is sending ACK to next hop and that hop sends ACK to its sender in the wake of sending packets to the neighbor. It may conceivable that at least two than two successive nodes may have same number of ACK. Sorting process at the sender side reductions the overhead and take out the issue of because of the substantial overhead.

6. PROJECTED ALGORITHM FOR PACKET LOSS REDUCTION

For every node decide the drop packets If packet dropped > edge include the nodes into pernicious node list if (every node is suspected)
{
node X checks ACK and sort them/X is the vindictive recorded node if (any ACK is lost from neighbor nodes)
{
check the ACK from destination comp(ACKneighbor, ACKdestination)
{
on the off chance that((ACK neighbor – ACKdestination)>=7) Add node into malignant node list
else
break;
}
}
}

7. RESULTS

The suggested method developed a MANET using NS2 simulator and results proved that the suggested method is far better than the existing method for secure routing and data transfer in MANET in the shortest path of the MANET.

Table 2. Parameters used for simulation

Number of nodes	100
Routing protocol	I-AODV
Area	1200*1200
Packet size	512 bytes
Mobility speed	0-50(ms)
Simulation time	300
Max no of connection	200
Tool	NS2

The proposed method uses I-AODV protocol and table.2 shows the parameters used in NS2 simulator.

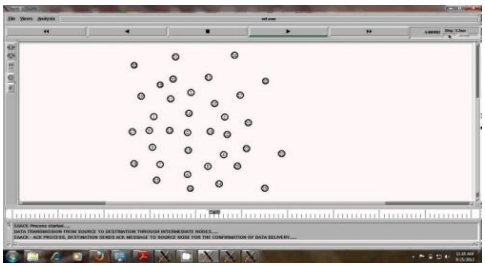

Figure 3. Creating of MANET

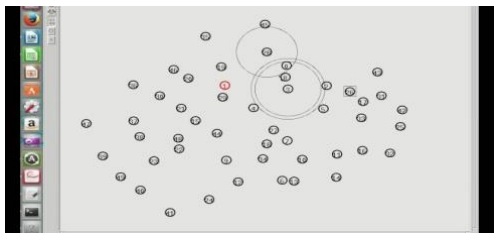

Figure 4. Multi-mode routing mechanism

Fig.3 and Fig.4 explains about the process of creating MANET and the performance of the multi-mode routing algorithm in which the PKG is used only when the number of nodes in the MANET is more than three and End-to-End cryptography is done if the nodes in the MANET is limited to two.

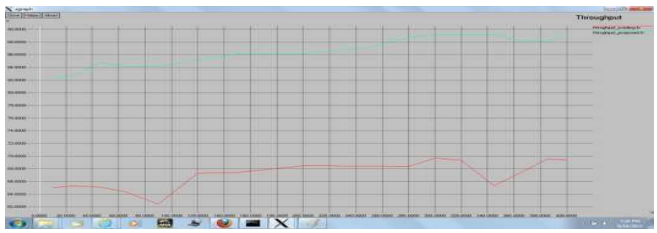

Figure 5. Comparison of throughput between existing and proposed method

The comparison of the proposed mechanisms with the existing method is illustrated in Fig.5 which proves that the existing method reduces the packet drop ratio.

8. CONCLUSION

In this paper, examination is done on the bad conduct of nodes and another approach is proposed for finding and confinement of acting up nodes. Here a new multi-mode algorithm is proposed which is used for secure routing and finding the shortest path among the MANETs and PKG is used for encryption and decryption process and the data is securely transferred among the MANET. It is finished up from the result that throughput is specifically affected by the packet drop in MANET. The 2-Ack based plan limits the overhead of the system and henceforth has constructive outcome on the execution of the network. To demonstrate the viability and after effects of proposed approach, usage deal with NS2 simulator.

REFERENCES

[1] Tyagi S. (2016). A reliablity based variant of AODV In MANETs: Proposal, analysis and comparison. Proceeding in 7th International Conference on Communication, Computing and Virtualization.

[2] Bhanumati V. (2012). RSS based energy EFFICIENT scheme for the reduction of overhearing and rebroadcast for MANET. Elsevier, Procedia Engineering 38: 2463-2472.

[3] Zhu QK. (2011). A mobile Ad Hoc networks algoritm improved AODV protocol. Proceedings of International Coneference on Power Electronics and Engineering Application.

[4] Yi L. (2003). Packet drop in mobile adhoc networks. Computer Science Technical Reports Paper, Purdue University 1558.

[5] Manish VM. (2014). Diminution of packet drop by efficient selection of network route in MANET. International Journal of Computer Science and Information Technology 5(2).

[6] Kaur A. (2013). Efficiency enhancement in AOMDV to reduce the chances of packet drop in MANETs. Proceeding of International Journal of Science and Research(IJSR) 2319-7064.

[7] Hassan ST. (2013). Designing a New MANET Environment using computer simulation. International Journal of Computer Science and Electronics Engineering(IJCSEE) 1(3).

[8] Ghosekar P. (2010). Mobile Ad Hoc networking:imperatives and challenges. Proceedings in IJCA Special Issues on “Mobile Ad-hoc Networks” (MANET).

[9] Sharma S. (2013). Reducing packet drop in MANET. Proceeding in Networkand Complex System.

[10] Srivastva SS. (2011). Minimization of the packet dropes in MANETS based on both static and dynamic routing protocols. International Journal of Computer Application (IJCA).

[11] Lanjewar A. (2013). Optimizing cost, delay, packet drop and network load in AODV routing protocol. Proceeding of International Journal of Computer Science and Information Security 11(4).

[12] Garg HK. (2012). Minimization of average delay, routing load and packet drop rate in AODV routing protocol. International Journal of Computer Application 44(15).

[13] Gaikwad S, Adane DS. (2013). Reduction in routing overhead using 2-ACK scheme and novel routing algorithm. IJETT 4(8).