ISSN- 2394-5125 VOL 06, ISSUE 04, 2019

Efficient Resource Utilization to Improve Quality of Service (Qos)using Path Tracing Algorithm in Wireless Sensor Network.

ANUVIDHYA G [1], VALARMATHY P [2], UMA R [3]

[1]Assistant Professor, Department of ECE,
[2]Assistant Professor, Department of CSE,
[3] Student, Department of ECE,
[1,2,3]DhanalakshmiSirinvasan College of Engineering and Technology, Chennai

ABSTRACT

Mobile Ad hoc Network (MANET) is a cluster of mobile devices capable of exchanging information wirelessly with each other without using a predefined infrastructure or centralized authority. MANET functions on the support of all the nodes participating in the network. The more nodes cooperate to transfer traffic, the more powerful a MANET gets.To successfully construct a Quality-of-Service (QoS) satisfied routing protocol with network coding, the bandwidth consumption of a coding host should be determined. Nevertheless, it is challenging to determine whether a host can be a coding host and to determine the bandwidth consumption of a coding host in a MANET. Sending packets from one device to another is done via a chain of intermediate nodes. Detecting routes and forwarding packets consumes local CPU time, memory, network-bandwidth, and energy. We find that the existing, Authenticated Routing for Ad Hoc Network (ARAN)uses Dynamic Source Routing (DSR) Protocol, whichmake greater performancecost. So we propose a novelty path tracing algorithm using Ad hoc On Demand Distance Vector (AODV) routing protocolfor finding the packet droppers in the MANET.The proposed Path Tracing Algorithm (PTA) also detects the Wormhole attack using per hop distance and link frequent appearance count parameters. The performance cost of the proposed method is minimal and outweighed when the security increases. As a result, there is a strong motivation for a node to denythe forwarding of packets to others, while at the same time using their services to deliver own data. In the course of broad experimentation we demonstrate that the proposed method avoids the Wormhole attacks, and the overhead required drastically decreases as the network size increases even it is non-discernible and hence the QoS is improved when compared to the existing ARAN protocol. The above proposed work is implemented using Network Simulator2 (NS2).

Keywords -ARAN, MANET, PTA,QoS, Wormhole attack and AODV

1. Introduction

MANET is a collection of mobile nodes and is able to communicate with one another in the absence of fixed infrastructure. MANETs are dynamic in nature and formed by independent mobile nodes. Each device in a MANET is allowed to move freely towards any path, and will consequently change its connection to different device much of the time[1,2]. Ad hoc nodes are wireless in nature and it is vulnerable to various wireless attacks. The primary challenge in building a MANET is preparing every device to continuously maintain the information required to appropriately route traffic.

ISSN- 2394-5125 VOL 06, ISSUE 04, 2019

Such networks may control by themselves or may be associated to the larger Internet. They support multi hop routing, an autonomous and decentralized administration, dynamic changes in network topologies, energy limited operation and network scalability[3].

Comparatively in MANET, reactive routing protocols perform well than the proactive routing protocol with reduced overhead to Wormhole attacks[4,5]. An independent feature of ad hoc node is responsible for the motivation of attacks. The nodes are allowed to move anyplace in a wireless environment and can join or leave any network at any time. These nodes are not fully secured and can be compromised, confined or hijacked by any attackers. There is no central authority and it is believed that all participating nodes are supportive in nature[6]. Many algorithms were proposed to ensure the node co-operation. The most important aim of the attacker is to destroy the cooperativeness of the ad hoc nodes**.** eavesdropping, wormhole attacks, denial of service etc.

To identify, track and show the negative effects that Wormhole nodes cause in MANET, we proposed Path Tracing algorithm to detect the Wormhole nodes using per hop distance and link frequent appearance count. To simulate the proposed work in NS2 regarding Quality of Service in MANET and evaluate through delay, packet delivery ratioand throughput.

Chapter 2 deals with literature review and existing system of the project. Chapter 3 deals with the existing problem. Chapter 4 deals with module description of the proposed work such as Packet Dropper In MANET, Packet Dropper Prevention And Detection and Estimate Packet Delivery .Chapter 5 deals with Network Simulator2 Software, performance analysis of existing and proposed mechanism. Finally chapter 6 deals with conclusion.

2. Literature Review

Joseph E. Mbowe and George S. Oreku[7] analyzed quality of service in wireless sensor networks based on Reliability,Availability and Serviceability(RSA) parameters rather than the traditional metrics and proved that the proposed mechanism works better than that of existing method.

Sapan Parikh, Amish Patel, and Syed Rizvi[8] proposed an improved quality of service method called timestamp Optimization technique. They presented both mathematical and analytical models to describe the proposed mechanism and it considers the sensor nodes that is having only one hop distance from the source to the sink.

Ajay Ramesh Karare, S.V.Sonekar and KumariAkanksha[9] proposed a SAFEQ and Watchdog algorithm to improve the quality of service in wireless sensor network. These two collaborative approaches provide Integrity, Privacy and Security to the wireless network and also prevents the networks from unwanted attacks. So the above proposed approach improves the quality of service.

A. Elakkiya, B. Santhana Krishnan and Dr. M. Ramaswamy[10] developed a quality of service approach named relative coordinate Rumour Routing protocol based on straight line random walk technique. The main intention of this paper is to calculate the performance metrics under various conditions such as position of a node , network size etc.

ISSN- 2394-5125 VOL 06, ISSUE 04, 2019

3. Problem Definition

Authenticated Routing for Ad hoc Network (ARAN) works on DSR, whichmakes a number of contributions to the design of secure ad hoc routing protocols. In reactive routing protocols, Detection and prevention of Wormhole Attacks in ARAN introduces authentication, message integrity, and non-repudiation to routing in an ad hoc environment[11,12].Here we are implementing packet dropping using DSR routing protocol. Almost all the protocols assume the existence of some routing security that guarantees that the selected route is free of malicious nodes. We find that although there is a greater performance cost to ARAN. Hencethe QoS is affected in the existing mechanism. So we propose a PTA for improving the Qos factors in MANET[13].

4. Proposed Mechanism

The proposed Path Tracing algorithm (PTA) will be structured into the following three main phases, which will be explained in the subsequent subsections:

- ☆ Packet dropper in MANET
- ☆ Packet dropper Detection and Prevention
- ☆ Estimation of packet delivery

4.1 Packet Dropper InManet

The Wormhole is one of the difficult attacks in the ad hoc routing in which two wormhole nodes creates a tunnel with high transmission connectivity referred as a Wormhole tunnel. The Wormhole tunnel may be wired or wireless.

As soon as Wormhole nodes initiate a malicious link, they start gathering the wireless information and forward it to one another. It is then relay the packets over the Wormhole tunnel to another location.

The legitimate data packets are relayed to some other place in the network and Wormhole nodes makes other nodes to believe that they are their immediate neighbors. The Wormhole attack affects both the proactive and on demand routing protocols. In this paper, AODV Protocol is used to analyze its performance in MANET during sending and receiving the packets and thus it is achieved by path tracing algorithm.

4.2 Packet Dropper Detection and Prevention:

This section briefly addresses system model, notations assumptions and unconsidered proposal. Packets are forwarded using source routing. Let us consider a collection of random mobile nodes consists of a set R={r1, r2, r3..., rn} that communicate each other through radio transmission and the neighboring node communicate each other in a bidirectional mode. For neighboring nodes, the distance between them should be less than a predefined distance ‘d’. We do not focus on assumptions on how the nodes are using MAC protocol to increase the access in radio transmission[14].

ISSN- 2394-5125 VOL 06, ISSUE 04, 2019

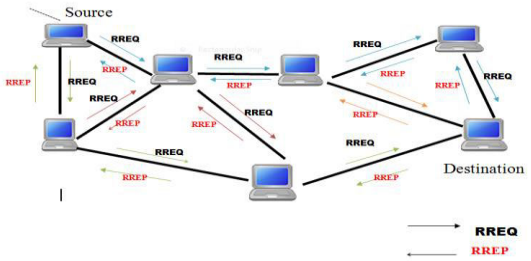


Fig..1 AODV Routing Structure

The network is designed in the manner of lose clock synchronization. Every node in ad hoc environment may or may not be resource controlled.The source node sends the Route Request (RREQ) packets through immediate neighbors towards the destination node[15,16]. When it reaches the destination, it sends back Route Reply (RREP) in the turnaround way. The path details are stored in the routing cache. In order to detect the Wormhole, we optimize the general packet header by adding extra fields. Prior per hop distance field and time stamp fields are added to the header of each packet. We consider both prior per hop distance and per hop distance so as to compare the difference between the two distances.

If the difference is too large that exceeds the maximum threshold value, then malicious is detected. All nodes are joined in the routing mechanism to perform this operation. The time stamp field is initialized at the time of the first bit of RREQ is sent. Per hop distance field can be changed by intermediary nodes but time stamp field cannot be altered by any other nodes. Whenever an intermediary node obtains RREQ, it calculates per hop distance with its immediate neighbor and compares it with the prior per hop distance in the header value.

After the comparison, it updates per hop distance in the prior per hop distance field in the packet header and forwards RREQ to its neighboring nodes. On obtaining RREQ, the receiver computes per hop distance with its neighbor in the reverse path and it places in the packet header. Every intermediate node forwards one RREP for each RREQ. Every RREP holds each hop distance of all path in which it is related. In addition to per hop distance value, it also holds the time stamp of the time taken between sending and receiving the RREQ and RREP correspondingly between two nodes. The computation of per hop distance of each node is described in the next section.

4.3 Per Hop Estimation:

The presence of malicious can be identified by calculating the distance between each hop in a path. We consider that per hop distance is calculated by using the Round Trip Time (RTT). RTT is defined as RREQ and RREP propagation time between the source and destination. Let us consider the RTT calculation between two nodes A and B where the two nodes are non-packet dropper nodes.

4.4 Variables used in RTT Calculation:

T rep: Time, when the first bit of RREP is received from B.

T req: Time, when the last bit of RREQ is transmit to A.

IPD: Intermediate node processing delay

By using formula, we can calculate the RRT between two nodes

ΔT= RTT= T rep – T req – IPD

ISSN- 2394-5125 VOL 06, ISSUE 04, 2019

4.5 Estimation of Packet Delivery:

After detecting packet dropper node, we need to take accurate measurements for packet sending and receiving and it is our responsibility to design an effective defense mechanism for malicious attack.

To achieve the goal, we propose to detect the malicious node using per hop distance and link frequent appearance count Parameters to develop the extension of AODV routing protocol[17,18].

With the estimated value of ΔT, per hop distance between A and B 'DAB' is considered by assuming the routing signals are travelling with the speed of light 'v'[19].

$$DAB = (v/2) * \Delta T.$$

Each node in the network has to perform four major operations to detect the packet dropper.

1. Compute per hop distance and compare it with the prior per hop distance.
2. Check whether the difference between prior per hop distance and per hop distance is larger than the maximum threshold value. If it is larger, then the packet dropper is detected and it is informed to all other nodes in the networks to provide packet dropper alertness. For the confirmation of packet dropper attack, the number of time a link is used in a path is also checked in addition to comparison of per hop distance.
3. If DBC - DAB >RTh and F Account >FATh then it is a packet dropper link.

Per hop distance is calculated at the time of route discovery to make our proposal energy efficient. Many routes are identified from the route discovery process. The packet header stores the per hop distance that calculate the each path of all the nodes. By comparing the per hop distance between all nodes in a path, a packet dropper can be detected. If the per hop distance exceeds the prior per hop distance through a maximum threshold range RTh. then the path related to that particular node is packet dropper.

4. For the effective packet dropper detection, we take another parameter called frequent appearance using Path Tracing Approach.If F Account > F ATh then it is a packet dropper link.After the detection of the packet dropper, a node intimates the presence of packet dropper to other nodes in the network. To prevent the packet dropper node participation further, their identities are added to the packet dropper list in each node. So that it is not necessary to calculate per hop distance each time when a path is discovered. Thus our proposed mechanism extends the computation energy by storing the estimated per hop distance in a cache. Hence the Quality of service has been improved in the wireless sensor networks.

4.6 Analysis of Frequent Appearance of a Link

In order to detect the malicious activity effectively, a link can be checked whether it participates in the routing very often. We can find frequent appearance (F Account) of a link (Lj) in a path by using the formula, F Account is equal to Maximum number of times that Lj participates in a path.F Account= N_j / Total number of available links in a path N

As there are many links in a path, it can also be used to detect malicious attacks. If a link in a path frequently takes place in routing such that its count exceeds the frequent appearance threshold (FATh), then it is a Wormhole link. The frequent appearance count information is collected only

ISSN- 2394-5125 VOL 06, ISSUE 04, 2019

through the monitoring and marked in cache.Our proposed mechanism is easy to implement with reduced overhead and requirements and does not rely on tight time synchronization. Every node should calculate RTT only using its own clock.

4.7 Path Tracing Algorithm(PTA)

Steps to detect the Wormholenodes in the Network.

Step 1: RTT values can be calculated based on the time between the RREQ sent and RREP received in a particular path . The RTT computation is calculated on the nodes own clock.

Step 2: Using RTT value, Compute per hop distance value. The calculated per hop distance value and time stamp are stored in each packet header.

Step 3: The above RTT information are stored to identify the Wormholeattack. Each and Every node in the routing path computes per hop distance with its neighbor and compares it with the previous per hop distance. If the per hop distance is greater than the threshold range, RTh, go to step 4.

Step 4: Check out the maximum count a link takes part in the particular route. If FAccount>FATh, then the link is Wormhole link.

Step 5: Mark the path as Wormhole and the corresponding node informs other nodes to alert the network. These Wormhole nodes are then inaccessible from the network.

5. Result and Discussion

The proposed Path Tracing algorithm for improving the quality of service in wireless sensor networkis implemented using Network Simulator2(NS2).In this simulator , 27 sensor nodes are performed in the region 700m x500mnam window. The results shows that the proposed path tracing algorithm produces better results in the parameters such as throughput, packet delivery ratio and the delay time.

5.1 Packet Delivery Ratio:

PDR is the proportion of the total amount of packets reached at the destination and amount of packet sent by the source. If the amount of malicious node increases, PDR also decreases gradually. The higher mobility of nodes causes PDR to decrease.

PDR = Total amount of data packet received (Destination) to the amount of packet sent (Source)

ISSN- 2394-5125 VOL 06, ISSUE 04, 2019

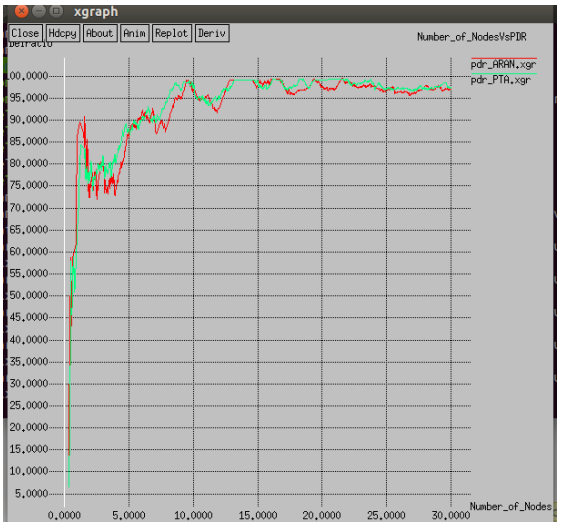
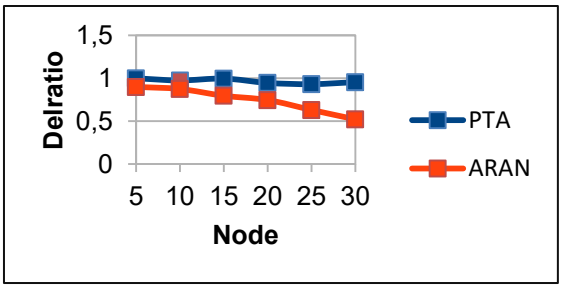
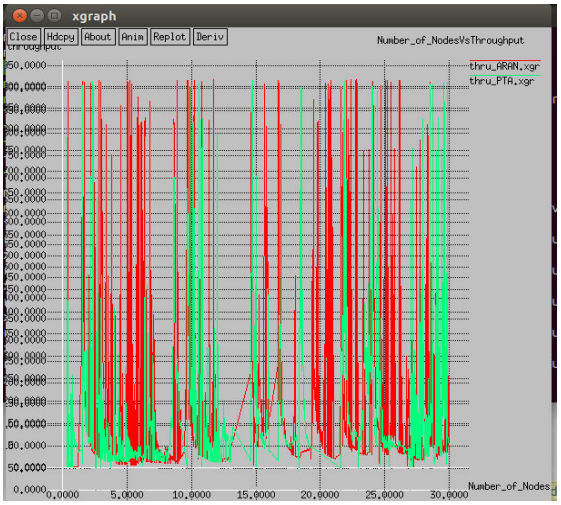


Fig.2 Nodes vs Packet Delivery Ratio



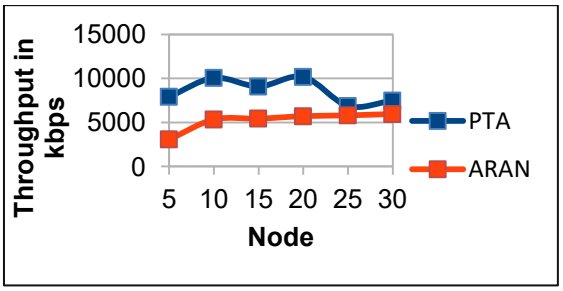
5.2 Throughput:

If the number of malicious node increases ,then the throughput decreases.The throughput of general DSR is 87% at the node mobility of 10 m/s for 10 malicious nodes and that of AODV is 95%. However the PT algorithm gives 97% of throughput.



No.of Nodes vs Throughput

ISSN- 2394-5125 VOL 06, ISSUE 04, 2019



5.3 Average Delay:

The average delay is the delay time that is calculated by measuring the elapsed time between the packet sent and received

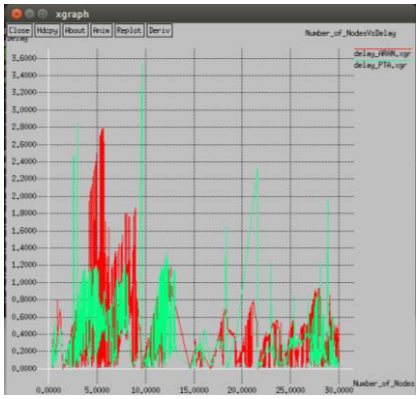
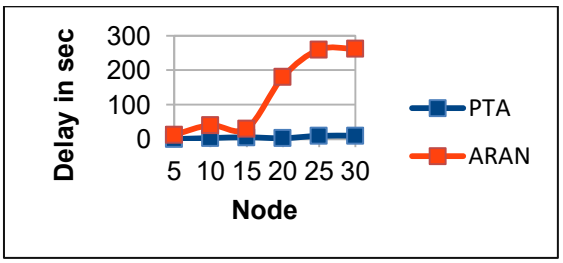


Fig.4 No.of Nodes vs Delay



6. Conclusion

In this reputation-based scheme, built on top of normal AODV secure routing protocol the malicious attack which is one of the network layer attacks (Wormhole). This initiates attacks by creating a tunnel between two or more Wormhole nodes and drops all the packets. To detect and prevent the Wormhole attack, we proposed Path Tracing algorithm (PTA). The proposed algorithm detects and prevents the Wormhole attack using per hop distance between two nodes and link frequent appearance count parameters. The simulation result clearly shows that our proposed algorithm is more effective in preventing the Wormhole attack with greater throughput and less average delay. The performance analysis of PTA has also reduced overhead and delay. Thus the Quality of service has improved while using the proposed mechanism and it doesn't need any additional hardware for implementation. Thus, the proposed design, proves to be more efficient and more secure than existing secure routing protocol in defending against both malicious and authenticated malicious node.

References

ISSN- 2394-5125 VOL 06, ISSUE 04, 2019

1. Tomur and Y.M. Erten, —Security and Service Quality Analysis for Cluster-Based Wireless Sensor Networks‖, Fifth International Conference on Wired / Wireless Internet Communications (WWIC 2007), May 2007, Coimbra, Portugal .
2. Vibhav Kumar Sachan, Syed Akhtar Imam and M. T. Beg, "Energy-Efficient Communication Methods in Wireless Sensor Networks: A Critical Review", International Journal of Computer Applications, Vol. 39, No.17, pp. 3548, 2012.
3. T.Rajesh and Prof.V.S.R.Kumari, "Design and Analysis of An Improved AODV Routing Protocol For Wireless Sensor Networks and OPNET", International Journal of Advanced Research in Electronics and Communication Engineering, Vol.3, Issue. 10, pp.1267-1278, 2014.
4. N. Sivakumar and Dr. G. Gunasekaran, ''The Quality of Service Support For Wireless Sensor Networks'', International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Issue.1, pp.297302, 2013.
5. Joseph E. Mbowe, George S. Oreku,” Quality of Service in Wireless Sensor Networks”Wireless Sensor Network, 2014, 6, 19-26 Published Online February 2014 (http://www.scirp.org/journal/wsn) http://dx.doi.org/10.4236/wsn.2014.62003
6. Sapan Parikh, Amish Patel, and Syed Rizvi,” Increasing Quality of Service (QoS) in Wireless Sensor Networks (WSN) by Using Timestamp Optimization Scheme”, ASEE 2014 Zone I Conference, April 3-5, 2014, University of Bridgeport, Bridgpeort, CT, USA
7. Mr. Ajay Ramesh Karare, Prof.S.V.Sonekar, Miss. KumariAkanksha “Improving the Quality of Services in Wireless Sensor Network by Improving the Security”, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 International Conference on Industrial Automation and Computing (ICIAC- 12th & 13th April 2014) .
8. A. Elakkiya B. SanthanaDr. M. Ramaswamy”Performance Evaluation of QoS Based Improved Rumour Routing Scheme for WSN”,International Journal of Wireless Communications and Networking Technologies Available Online at http://warse.org/IJWCNT/static/pdf/file/ijwcnt01522016.pdf.
9.] R. Iyer and L. Kleinrock, —QoS Control for Sensor Net- works,‖ in ICC 2003, Vol. 1, 11 -15 May 2003, pp. 517-521.

   M. Sharifi, M. A. Taleghan and A. Taherkordi, —A Mid- dleware Layer for QoS Support in Wireless Sensor Net- works,‖ Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, Mauritius, 2006.

ISSN- 2394-5125 VOL 06, ISSUE 04, 2019

10. Sung-Keun Lee, Jin-GwangKoh and Chang-Ryul Jung, "An Energy-Efficient QoS Aware Routing Algorithm for Wireless Multimedia Sensor Networks", International Journal of Multimedia and Ubiquitous Engineering, Vol.9, No.2, pp.245-252, 2014
11. Wang Jietai, Xu Jiadong, and Xiang Mantian, '' Eaqr: An Energy-Efficient Aco Based QoS Routing Algorithm in Wireless Sensor Networks", Chinese Journal of Electronics, Vol.18, No.1, pp.113-116, 2009.
12. Prabha R, ShivarajKarki, Manjula S. H, K. R. Venugopal and L. M. Patnaik, "Quality of Service for Differentiated Traffic Using Multipath in Wireless Sensor Networks", International Journal of Inventive Engineering and Sciences, Vol.3 Issue.1, pp.61-66, 2014.