ISSN:0975-3583,0976-2833 VOL10,ISSUE04,2019

A New Thresholding based Approach for Wormhole Attack Prevention in MANETs

Saroj KumarRout[1], Nibedita Sahoo[2], Sasmita Pani[1]
[1]Professor,[2]Assistant Professor, [1,2]Dept. of CSE
[1,2]Gandhi Institute for Technology, Bhubaneshwar, India

Abstract

In real time environment, the nodes in a mobile ad-hoc network (MANET)moves actively. There will be many attacks in network layer which lead to the performance degradation of the wireless network. Among them wormhole attack causes serious problems which will affect the owl MANET system. Wormhole attack can be defined as a created tunnel from more than one malicious node. Here, we proposed a new approach for preventing the wormhole attack by utilizing the threshold algorithm (NWATP-TA). Our proposed algorithmnotices these sorts of attackeffectively in MANET systems. Experimental analysis shows that the robustness of the proposed approach over the conventional wormhole attack prevention schemes in terms of throughput, end-to-end delay and energy consumption. We also compared our results with the Trusted AODV protocol.

Keywords: Mobile ad-hoc networks, wormhole attack, AODV routing protocol, trusted AODV routing protocol,

1. Introduction

A mobile ad-hoc network (MANET) is wireless network that means it's not recurred infrastructure. In MANET nodes are move energetically nature. The dynamic natures of MANET make it more vulnerable. In network layer many attacks possible but we focus only wormhole attack. When more than one malicious node creates tunnel is called wormhole attack. In ad-hoc network, routing is a vital challenge because of node's high mobility. Trust-based routing is being defined in our proposed approach, which calculates the value of trust based on the hyperbolic function of tangent that computes the trust value of their adjacent nodes promiscuously.In MANET, there is no fixed infrastructure therefore the mobile nodes communicate over multi-hop wireless links. These are often cited as infrastructure-less network model because the mobile hosts in the network establish route between themselves. Caching has been proved to be a very important method for improving data recovery and performance in mobile communication area. Caching, data or information process delay is minimized since queries or requests are served from the local cache there by clearing the need for data transmission.There are several attacks in an unexpected network. referable to their open nature, mobile ad hoc networks systemnonresistant to most of the attacks such as gray hole, denial of service, wormhole, black hole, Sybil etc. Among these attacks, wormhole attack detection is a challenging and difficult tasksince this attack detection doesn't need any skill violation by the user. In a network location, one venomous node register traffic and then that traffic will be tunneledto a various venomous node that is found far in other location which is known to be distribution of routing. It's very crucial and important to detectsuch attacks in MANET systems.Various routing protocols in [1-5] presented in the literature, which provides the transmission of data from the source to destination with a best effort. These

protocols work proactively or reactively and find a minimum hop path from source to destination. Route discovery and route maintenance procedures incorporate node mobility and are kept simple to impose minimal routing overhead on the network. Nodes in an ad hoc network are equipped with batteries and are usually mobile with varying node speeds. Inefficient utilization of battery energy via increased load (i.e. data transmission) on nodes may disrupt communication as nodes may die sooner due to energy depletion. Also, traditional routing protocols quickly discover a single route towards destination and source forwards data via this route. In case of abrupt link failures due to mobility or errors in wireless transmission on the discovered path a new route discovery is initiated leading to increased delays. The above-mentioned issues can be facilitated by disclosingthe multiple directions to the destination, which can be stored at the source node or at the in between nodes and can be utilized immediately in case of any failure happens in the nodes link.

2. Related Work

In [6], proposed a CTPKM with no central trust entity with the goal of maximize presentation, at the same time as justifying security liability. Each node provides a trust threshold to determine whether or not to trust another node. Each node's choice creation using the known trust threshold affects presentation and security of CTPKM. Author take three different parameters competence, integrity, and social contact on the basis of this parameter set the trust level.In [7] author proposed a method based on route redundancy, route aggregation and round-trip time There are three phases on which proposed algorithm works in first phase, create a multipath to authenticate RREQ, second phase is used to aggregate which help to know the all possible paths of the source and destination. In last phase there is calculation of average time of all routes based on the number of hopes.In [8] author proposed a technique called PAWAODV (Power-Aware AODV) these techniques help to enhance the performance of device which has limited power resources and with help PAW-AODV devices can perform better as compare the normal AODV, Hop-Count limit is also a factor which helps to choose the efficient path.

2.1. Trusted AODV routing method

Trusted AODV is a trusted routing protocol based on trust model for mobile Ad-hoc network. Trusted AODV has many relevant features like Nodes perform trusted routing behaviors mainly according to the trust relations between them. A node that performs malicious behaviors will finally be detected and denied to the entire network. System routine is improved at every routing hop. Here the AODV routing protocol is embedded along with the trust function. The communication between the nodes in the mobile Ad-hoc network depends on the cooperation and the trust level with its neighbors. Based on the trust on neighbor and appropriate threshold values the nodes be capable of be categorize in to the subsequent.The conditions of node level:

Unreliable: it's having trust value between 0 to 0.5.

Reliable: it's having trust value between 0.4 to 0.7.

Most Reliable: it's having trust value between 0.7 to 1.

3. Proposed System

In this paper, we propose a new method named as Wormhole attack prevention-threshold algorithm and it is described as Wormhole nodes and are announced to all other nodes. All nodes remove wormhole node id from its neighbor table and routing table. If any forwarding node receives the wormhole announcement node, it will send RERR message to source. It will reinitiate route discovery process and find the new path to the destination without wormhole node.

3.1. Algorithm

Step1: whenever a source node needs a route to destination the protocol starts route discovery. During route discovery, source node broadcasts RREQ packets through neighboring nodes. RREQ packet contains destination address and sequence number along with source address. Sequence number provides the freshness of the route.

Step2: once an RREQ packet is received by an intermediate node and verifies destination address. If the destination address not matches with the RREQ packet, then forwards it to its next hop. This process is repeated until it reaches the destination.

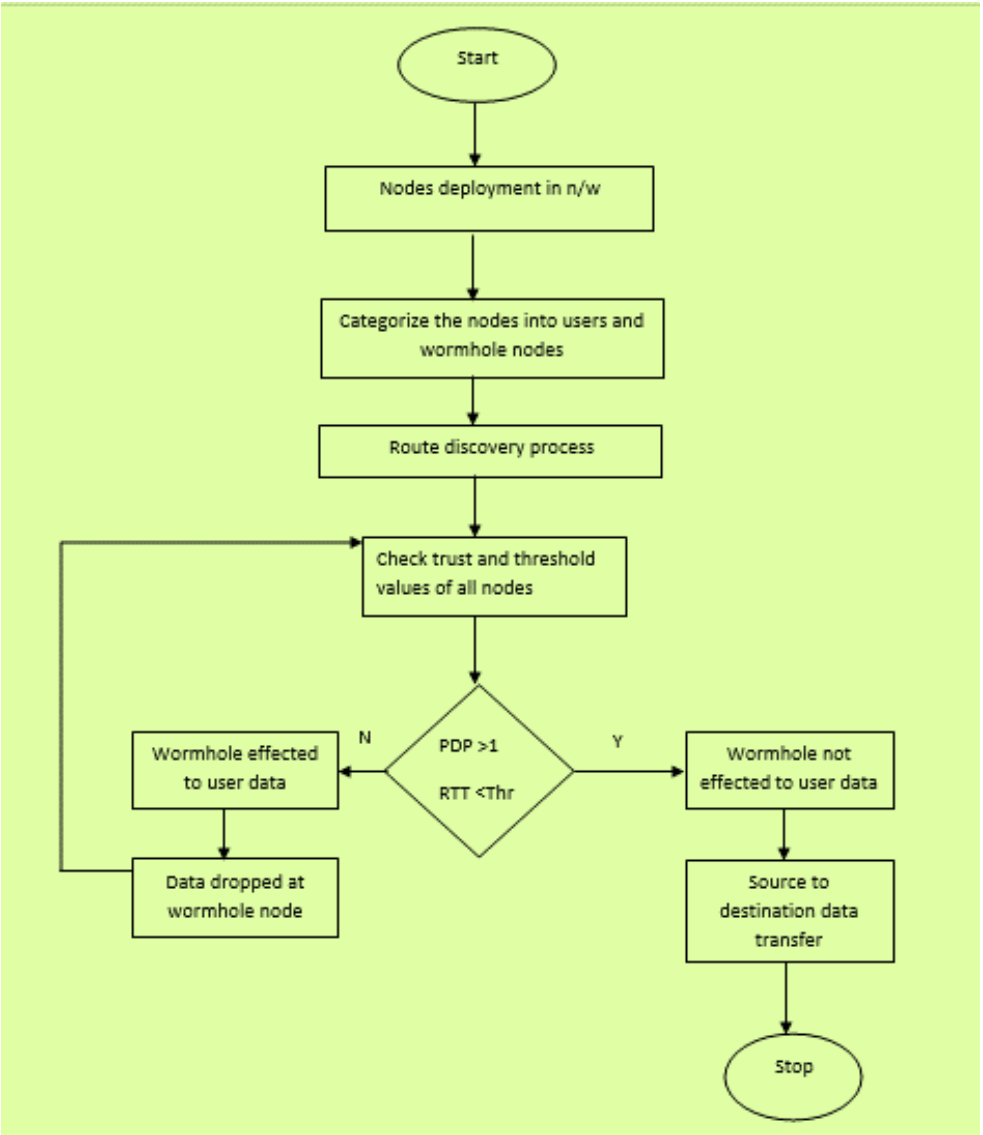

Figure 1. Flowchart of proposed algorithm

Step3: route path nodes are saved in routing table.

Step4: when source node starts sending packets, it sends to next node and that node sends to next until it reaches destination. The traversed path nodes are checked with the path nodes in routing table.

Step5: if the traversed path nodes are not in the routing table, wormhole is detected, and it is out band wormhole.

Step6: while sending packets to next neighbor node, PDR is calculated for each node. the ratio of sent packets to received packets is calculated for each node.

Step7: Hello packets also sending to each node along with packets until it reaches destination. Roundtrip time is calculated for each consecutive node. if the roundtrip time is less than threshold, that link is high speed link and the two nodes are malicious and detected as wormhole. And, if the PDR is less than 1, that node is wormhole node. the wormhole detected is active wormhole as it affects the packets.

Step8: If PDR less than 1 and RTT is not less than threshold means the loss may be due to traffic.

Step9: If PDR not less than 1, check for RTT less than threshold or not. If it is less passive wormhole is detected as the packets are not affected. If it is not less than the threshold, there is no wormhole.

Step10: Wormhole nodes are announced to all other nodes. All nodes remove wormhole node id from its neighbor table and routing table. If any forwarding node receives the wormhole announcement node, it will send RREP message to source. It will reinitiate route discovery process and find the new path to the destination without wormhole node.

4. Simulation Results

This section describes the simulation analysis of our proposed approach with comparison to the existing wormhole attack nodes prevention such as trusted AODV and normal AODV routing algorithms. We performed our test results in network simulator 2 (NS2) under the specifications provided in simulation table 1.The figure 2 shows that the analysis of throughput in which the simulation time has considered as X-axis and in Y-axis we took throughput values. We can observe that the performance of our proposed algorithm enhances the value of throughput when we compare with the Trusted AODV routing algorithm and normal AODV method.Figure 3 and 4 shows that the performance analysis of end-2-end delay and energy consumption, which provides that the superiority of our proposed wormhole attack nodes prevention algorithm.

Table 1. Simulation parameters

Parameter	Value
Application traffic	CBR
Transmission rate	10 packets/sec
Radio range	250m
Packet size	512 bytes
Channel data rate	10Mbps
Maximum speed	30m/s
Simulation time	10secs
Number of nodes	25
Area	1000x500
Wormhole nodes	4
Routing protocol	AODV
Threshold	Dynamic threshold

ISSN:0975-3583,0976-2833 VOL10,ISSUE04,2019

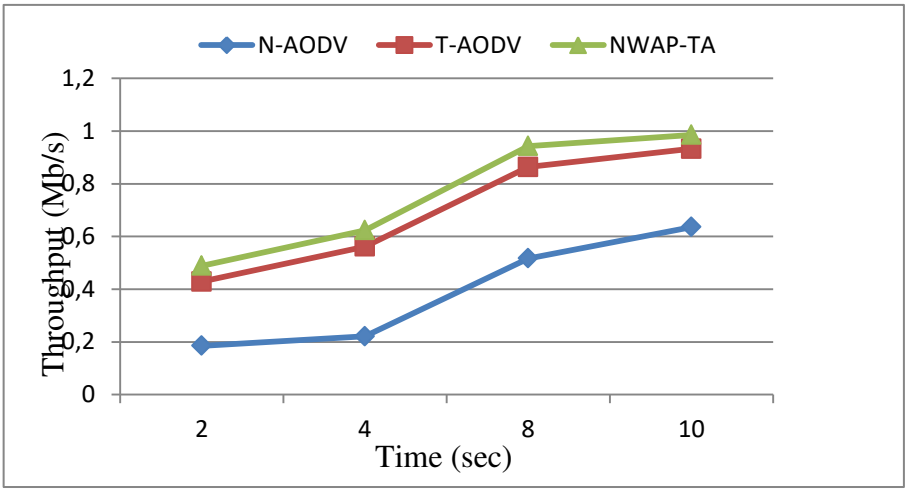

Figure 2. Comparative analysis of throughput with proposed and conventional routing algorithms for wormhole prevention

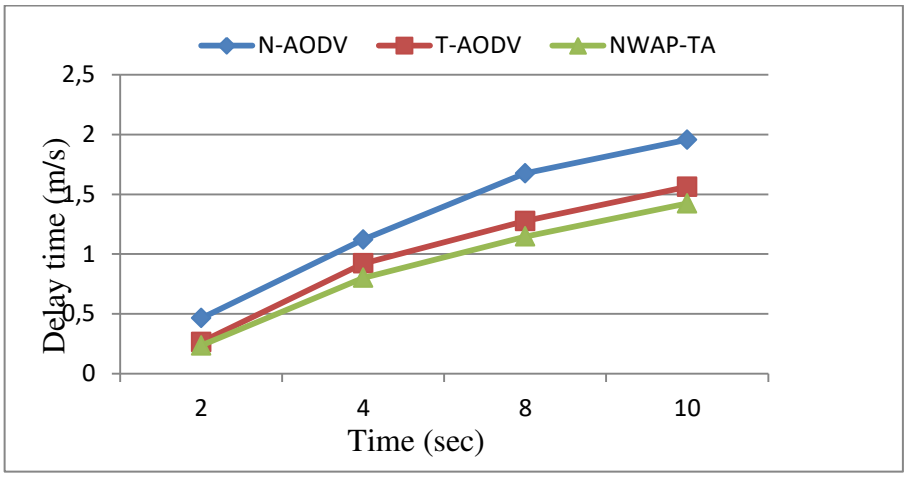

Figure 3. performance analysis of end-2-end delay

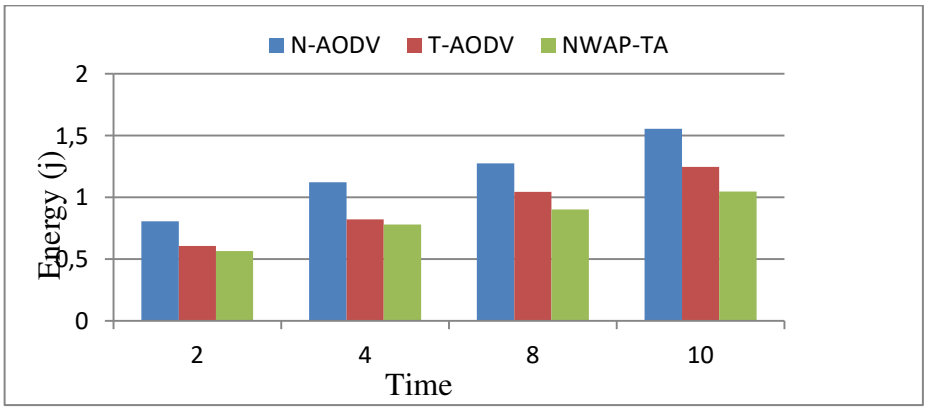

Figure 4. Comparative analysis of energy consumption with proposed and conventional routing algorithms

ISSN:0975-3583,0976-2833 VOL10,ISSUE04,2019

5. Conclusion

In this paper, we focused on detection and removal of wormhole attack during data transmission. The proposed algorithm provides more security to ad hoc networks and also prevent from such kind of attacks. It helps to increases the packet delivery ratio and reduces the control overhead by improving the performance of the routing protocol. Here we are discovery following conclusion on NS-2simulation. Like End to end delay of new fresh algorithm is better compare to TAODV. In future, we also plan to improve the table entries at destination node to get the detection of wormhole nodes faster. And also improve the security of wireless ad hoc networks. By deploying such efficient methods to prevent DoS attacks and hybrid attacks with the help of Wormhole attack prevention threshold algorithm.

References

[1]. ASharma, D bhuriya, U singh , "Secure data transmission on MANET by hybrid cryptography technique", IEEE 2015 International Conference on Computer, Communication and Control (IC4), pp. 1-5, 2015.

[2]. Jin-Hee Cho, Kevin S. Chan, Ing-Ray Chen et al., "Composite Trust-based Public Key Management in Mobile Ad Hoc Networks", ACM 28th Symposium on Applied Computing, pp. 1949-1956, 2013.

[3]. Reshmi Maulik and Nabendu Chaki "A Study on Wormhole Attacks in MANET", International Journal of Computer Information Systems and Industrial Management ApplicationsISSN 2150-7988, Vol. 3, pp. 271-279, 2011.

[4]. C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On demand Distance Vector (AODV) Routing," IETF RFC 3561, pp. 1-11, 2003.

[5]. Isaac Woungang, Sanjay Kumar Dhurandher, Mohammad S. Obaidat, Issa Traore et al.,"Timed And Secured Monitoring Implementation Against Wormhole Attack in AODV-BasedMobile Ad Hoc Networks", IEEE, pp. 1-5, 2013.

[6]. Jin-Hee Cho, Kevin S. Chan, Ing-Ray Chen et al., "Composite Trust-based Public Key Management in Mobile Ad Hoc Networks", IEEE, 2014.

[7]. Soo Young Shin, Eddy Hartono Halim eet al., "Wormhole Attack Detection in MANETs using RouteRedundancy and Timebased Hop Calculation", IEEE, 2012.

[8]. Chee-Wah Tan, Sanjay Kumar Bose,et al.,"Modifying AODV for Efficient Power-Aware Routing in MANETs", IEEE, 2007.