ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

TAEACK: A Time Adaptive Enhanced ACK Mechanism for Detecting and Preventing Sink-Hole Attacks in MANET

[1]G. Venkata Swaroop, [2]Dr. G. Murugaboopathi, [3]S.A. Kalaiselvan

[1]Research Scholar, Department of Computer Applications, St. Peter's University, Avadi, Chennai, Tamilnadu, India.
[2]Associate Professor, Department of Computer Science and Engineering, Kalasalingam University, Srivilliputtur, Tamilnadu, India.
[3]Research Scholar, Department of Computer Science and Engineering, St. Peter's University, Avadi, Chennai, Tamilnadu, India.

ARTICLE INFO

Article history:
Received 23 June 2015
Accepted 25 August 2015
Available online 2 September 2015

Keywords:
Sinkhole Attack; Secured MANET; Acknowledgement; Malicious Node; Data Transmission.

ABSTRACT

Nowadays Mobile Adhoc Network is growing drastically for wide range of communication. Nodes in MANET are created and deployed randomly, as well as nodes having mobility in nature. Since the nodes in MANET having mobility it is difficult to analyze the next hop individualities dynamically in the route. Possibilities are high for any one of the end node in the pair wise communication may be a malicious node. Where the malicious node collects all incoming data and possesses all the data and this kind of node behavior is called as Sinkhole attack. To avoid sinkhole attack an acknowledgement based and enhanced acknowledgment based approaches were discussed earlier. In this paper a Time Adaptive Enhanced Acknowledgement [TAEACK] approach is proposed to find and discard malicious node in the route. TAEACK approach will send and receive the acknowledgement before and after data transmission among the pair of node within a time interval and distance, Security-Key verification. Where the nodes location are estimated and computed by ALWadHA approach. TAEACK is more efficient than earlier approaches. The simulation result shows the proposed approach efficiency.

© 2015 AENSI Publisher All rights reserved.

To Cite This Article: G. Venkata Swaroop, Dr. G. Murugaboopathi and S.A. Kalaiselvan., A Time Adaptive Enhanced ACK Mechanism for Detecting and Preventing Sink-hole Attacks in MANET. ***Aust. J. Basic & Appl. Sci.,*** *9(27): 291-299, 2015*

INTRODUCTION

Today rapidly growing network technologies more sectors understand the merits and demerits of computer networking. The networks are made by fixed or temporary connections. Fixed connections are made up of cables. This connection is also called as wired connection. And the second one is temporary connection are made of modems. In recent years, wireless ad-hoc network playing a major role in communication networks. An ad-hoc network is a local area network (LAN) is built spontaneously as devices connect. A MANET is one type of ad-hoc network and this network infrastructure less. It has no base station and it has no fixed network infrastructure. It can change the location and configure itself during run time. This can be a standard Wi-Fi connection or another medium, such as a cellular or satellite transmission. Nodes in these networks will generate both user and application traffic and carry out network control and routing protocol. The advantages of MANETs are, self-configurable, cost effective, it consumes less time, more robust than cellular system, mobility and rapid deployable.

Attacks in MANET:

Attacks can be classified into active and passive. In active attack the attacker attempts to modify the data being transmitted in the network. In passive attack the attacker generally used to gather the information about the network. Some of the attacks are black hole attack, wormhole attack, Byzantine attack, resource consumption attack, flooding attack, sink-hole attack, etc.

Sinkhole Attack:

Sinkhole attack is one of the dangerous attacks in mobile ad-hoc networks. In sinkhole attack a compromised node attracts all the traffic from its neighbor by revealing that it has a shortest path to base station after that it collects the data. There are various security issues and challenges are discussed in various papers and some of the discussion is given in the related works.

Corresponding Author: G. Venkata Swaroop, Research Scholar, Department of Computer Applications, St. Peter's University, Avadi, Chennai, Tamilnadu, India.
E-mail: venkataswaroop.g@gmail.com

Background Study:

A secured data binding with the people was obtained by secure name resolution in (Javad Pashaei Barbinand, 2013). It was independent on the system names and it can be used with any earlier designed identification scheme to improve the security of name resolution even if the link failure or in the offline. An efficient position-based opportunities petal routing protocol is proposed in (Johnsi, J., G. Abija, 2013), which uses stateless property of the geographic routing and the broadcast nature of the wireless medium for mobility based nodes. An energy efficient topology control problem was proposed (Krishna K. Pandey, 2013) for co-operative communication which uses the optimum relay nodes selected for CC network. It reduces the energy consumption in the network. In (I-Wei Lai, 2013), two coding schemes were proposed for a virtual MIMO scenario which can enhance the end-to-end communication, and it is reliability by exploiting the path delivery. VANET architecture and the relevant protocols with the corresponding applications are discussed in (Saif Al-Sultan, N.,). Same VANET is introduced with data collection and aggregation based real-time speed with the position information on the separate vehicles. Also in this paper (Kartik Pandit, 2013), the signal is optimized to control the traffic intersections with the help of OAF and OJF algorithms. A decentralized algorithm is proposed for message forwarding in (Rene L. Cruz, 2013), and the author considers a novel message format for message transmission. Various routing protocols are proposed for MANET, helps to choose the appropriate routing protocol for various networks according to the network conditions. Paper (Dhenakaran, S.S., A. Parvathavarthini, 2013) provides a detailed discussion of various routing protocols which gave a comparative study among the protocols. Security for genuine nodes can be obtained by providing a secure privacy preserving approach in (Muthumanickam, Kandhasamy, 2013). Whenever a node communicates to other node, they should prove the confidentiality for secured communication. A BFD-[Bellman-Ford-Distributed] algorithm and k-shortest path algorithm is applied to find a better solution for ASWP problem in the network (Sasikala, G., L. Rajalakshmi, 2013). This also can be achieved by utilizing the TDMA scheduling method to improve the bandwidth, delay and throughput of the network to provide QoS.

In (Renato M. de Moraes, 2013), a new communication scheme was introduced, based on the co-operative MIMO–MANET, where this network has M antennas connected with the end users. The nodes under Receiver Consensus, they can autonomously achieve agreement for forwarding the strategies discussed in (Junliang Liu1, 2013). (Pietro Michiardi and Refik Molva, 2001) Provides a detailed study about the security issues in MANET and relevant threats affecting the performance of the network under DSR protocol. A watch dog based security s provides with pathrater to eliminate or avoid malicious nodes in the network is proposed in (Sergio Marti, 2000).The malicious node activities are detected by various IDS, cooperative-IDS, watchdog and pathrater is briefly explained in (Isha V. Hatware, 2012). The most recent safekeeping standard, 802.11i, allows for the amalgamation of such roaming endorsement methods, which may be based on public-key certificates or other testimonial. EAP was proposed for apply with the PPP protocol in Blunk *et al.* In Aboba *et al.* discussed the TLS expansion for EAP. Rigney *et al* formed the present RADIUS standard. Then, Rigney *et al.* (2012) discussed EAP as a RADIUS enlargement. Stanley et al describe necessities for EAP methods used in IEEE 802.11 wireless LAN in (Aboba, B. and D. Simon, 1999). But in this paper to overcome the time, more number of keys, wastage of memory the TAEACK method is proposed and shows the simulation result for better performance in security.

Problem Statement:

Due to dynamic and random nature of node deployment in MANET there is a possibility of various packets dropping attack. In MANET the source node sends the data packet with the help of intermediate nodes. Here the security mechanism is essential for ensuring the behaviors of the nodes and availability in the route. TAEACK provides detecting and preventing sinkhole attack by investigating the node-ID, location and TTL with the security Key and it is shown in Figure-1.

System Model:

The overall system model simulated for TAEACK is shown in figure-1. It shows the source node, destination node and the intermediate nodes in a route for data transmission. Next hop selection, location estimation and route selection is given clearly in the above figure.

Proposed Approach:

TAEACK concentrates on the REQ-TIME [request time], RES-TIME [response time], and compute the distance using the location of each node in the route. The location of the nodes are estimated and compared with the computed distance with the help of ALWadHA approach. This process confirms that the nodes location, original distance among the nodes by applying Euclidean formula.

Network Model:

Network G consists of K number of nodes. Source node Stransmits the data packets to the destination node$D$.Where$\{n_i, n_{i+1}, \ldots\ldots, n_k\}$, is k numbers of nodes are available in the route between S to D. Before transmitting the data to D the route construction will be carried out by investigating entire nodes on the route from S to D. The network

area is imagined in a rectangular shape and the entire network is divided into sub regions in column wise depicted in Figure-2 and it is treated as levels from the source node to destination node. Each level of the network consists of many nodes and the source node initially sends a REQ packet to the next hop from its position and receives ACK message. Each packet sending time and the ACK receiving time are calculated. It is assumed that the node one who is taking less ACK time will be treated as the next neighbor node and their approximate distance also calculated.

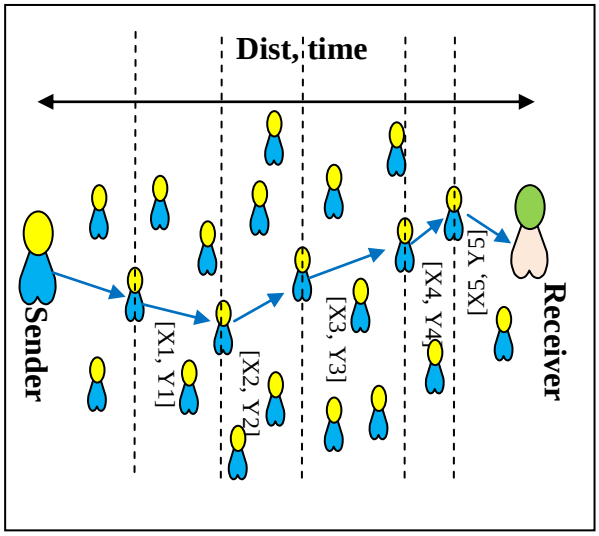

Fig. 1: Proposed System Model.

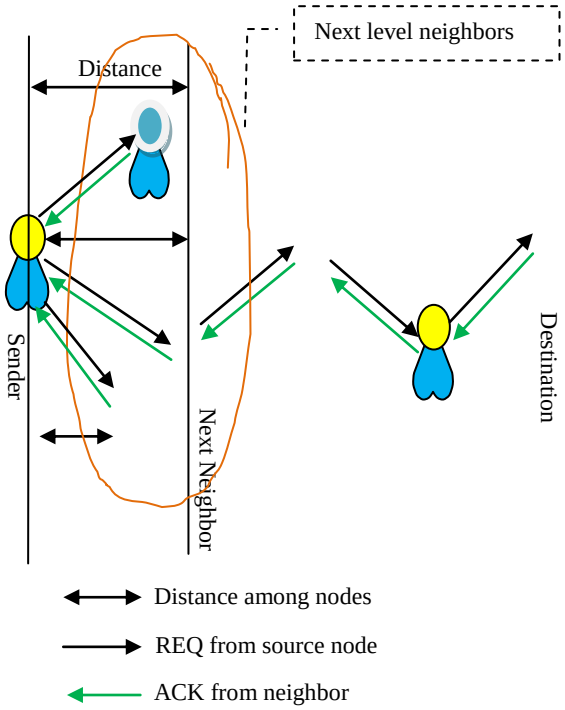

Fig. 2: Neighborhood Management for Route Discovery.

While REQ sent to the next level nodes, the ACK is received from all the nodes available in the next level. The ACK message is provided with the TTL, node ID and location. The ACK time and distances is computed for choosing the fast replied and less distance based node as the next neighbor node and mark it in a table. The distance among the nodes can be obtained by the bandwidth, local node time; remote node time using the corresponding equation-1 is given below.

$$\textbf{distance} = \frac{[speed \times t_{remote} - speed \times t_{local}]}{2} s/m$$

--Equation [1].

Where,

$\boldsymbol{distance}$ →is the distance among nodes
$\boldsymbol{t_{local}}$ → is the time of the source node $[S]$
$\boldsymbol{t_{remote}}$ → is the time of remote node $[D]$
$\boldsymbol{speed}$ → is the bandwidth of the data transmission

According to the distance the location of the neighbor node will be calculated using

$$[\boldsymbol{x_{remote}}, \boldsymbol{y_{remote}}] = [\, \boldsymbol{d - x_{local}}, \boldsymbol{d - y_{local}} \,]$$

--Equation [2].

Once the distance, locations are calculated it is stored in the [R_{TABLE}] for future reference after comparing the location with the estimated location using ALWadHA approach. The location of the neighbor node is estimated by nearest reference method using ALWadHA algorithm. In this algorithm a set of nodes are taken as a reference set, where the location of the reference set is already predefined or those nodes are initiated as Beacon nodes. The nearest reference method increases the accuracy of the location estimation.

This nearest reference approach is an easiest approach, where a set of nearest neighbors are chosen as a subset to compute the position of each nodes. The position of the neighbor node is computed by selecting nearest 3 beacon nodes and by APS computation method [i.e. triangulation method]. Any attacker provides incorrect location reference to the other nodes it can be find out by ALWadHA approach whether the location is correct or not.

Table 1: R_{TABLE}

SEQ.NO	NODE-ID	DURATION	LOCATION	Node-Key
1	2	5sec	120, 140	Uu
2	6	4sec	130, 160	Uu
3	7	7sec	210, 170	9
:	:	:	:	:
K	I	M sec	X, Y	Uu

The complete functionality of the proposed approach is given in stages as

- ✓ Node Registration
- ✓ Route Discovery
- ✓ Data Routing
- ✓ Cross verification by Location Estimation.

All nodes in the network are assigned by an ID [starting with Single digit random umber] and the location of the birth place X, Y. In the entire network the number of nodes in the first level is assumed as single node named as S [i.e. source] and from the next levels the number of nodes is K. In the initial process the node S sends REQ message to all the nodes in the first next level and receives RES message separately from those nodes and compute the time using TTL of the message sending time and receiving time. It chooses the next nearest neighbor and updates its information into routing table with REQ-RES time. The above process repeated to find next neighbors for the route until reaching the destination node and update the information about these nodes [ID, TTL, Location] in the routing table.

To provide more security a Key is generated for entire node available in the route while route discovery and updated in a $\mathbf{R_{TABLE}}$. While data transmission the entire node available in the route information is verified for validating the nodes in terms of TTL, ID, X, and Y values. The key is generated for each node in the route dynamically while route discovery and it is obtained by Equation-[3].

Key $[\boldsymbol{Node_i}] = \boldsymbol{append}[\boldsymbol{Node_{ID}}, \boldsymbol{hopcount}]$ - Equation [3]

For example:

Key (Node-7) =append [7,2] = 9 is the key for Node-7.

Node-7 is one of the intermediate hop in the route. Where node-7 is discovered as 2nd hop node in the route. Since the key of node-7 is 7 + 2 = 9. The same way the node security Key are generated and assigned to intermediate nodes and updated in the R_{TABLE}.

While data transmission the node information is cross verified by providing Node-ID, TTL and location to the next-hop with the $R_{TABLE.}$ Once the route discovery process is completed successfully, the source node 'S' start sending the data packets though the nodes in the routing table, by comparing their information once again with the routing table and pass the data. If the node submitting information is not matching with the routing table information, the node will be detected as malicious node and eliminated from the network and broadcast about the malicious information to all other nodes in the network for further security.

$$\boldsymbol{packetsizeis \rightarrow p}$$
$$\boldsymbol{numberofpacketis \rightarrow pn}$$

$\boldsymbol{t_0}$ →time of packet delivery at node0 to node1
$\boldsymbol{t_1}$→time of packet received at node1 from node0
Then $\boldsymbol{t = t_0 - t_1}$ **and the distance among the node is** $\boldsymbol{d = p * Pn \,/\, t}$

If the distance computed is not accurate then the location of the node is not submitted correctly by the reference node or the malicious node is not providing all the information correctly and especially the location. So that location can be computed and estimated accurately by the Location Estimation algorithm ALWadHA for suspecting nodes.

Location Estimation:

For estimating and computing the location of nodes, some of the nodes are assumed as special nodes named as beacons which are need for location discovery. Beacon nodes are getting their location with the help of GPS receiver or by manual configuration. The remaining nodes can compute their location with the help of beacons and currently their location are called as unknowns. There are three necessary components such as angle or distance, position estimation and a localization algorithm available in a localization system.

Some of the nodes are always trustable nodes in a network, as same some nodes are assumed as trustable beacon nodes in this paper. Since beacon, the nodes know its location by itself and they broadcast their location to the other nodes while transmitting messages. Using these characteristics of the beacon nodes, all the nodes location is computed accurately in the beginning stage itself. This location is used to verify and compared with the nodes submitting locations whenever it is needed. For various states like receiving a data packet, transmitting a data packet, idle, listening and sleep, wakeup different amount of energy is reduced from the initial energy of the node. Those energies are updated in each round of the data transmission. The initial energy is initialized as 100 joules. And for each state some amount of energy is predefined and assigned.

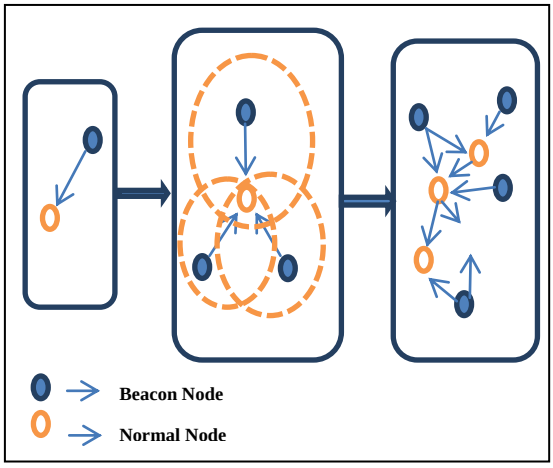

Fig. 3: Localization system using ALWadHA Model.

Initial Energy = 100 joules
Transmitting Energy = 0.26 joules
Receiving Energy = 0.08 Joules
Idle Energy = 0.01 Joules
Sleep Energy = 0.005 Joules
Wakeup Energy = 0.005 Joules
In each round the initial energy is updates using the following formula like

$$Initial_Energy = Initial_Energy - [TransmittingEnergy + ReceivingEnergy + SleepEnergy + WakeupEnergy + IdleEnergy + ListeningEnergy$$

Algorithm TAEACK( )
{
1. Network G = {$n_1, n_2, n_3, \dots\dots\dots, n_N$},
BS is the Base station
2. For I = 1 to N
a. Key(N_i) = append[Node-ID, hop count]
3. End
4. For J = source to destination
5. If (Key[$Node_i$] == $Key - table - row[i]$) then
6. If (Node-ID . exist(R_{TABLE}) then
7. If (Node-X, Node-Y . exist(R_{TABLE}) then
8. $data(Node_{i+1}) = data(Node_i)$
9. Else
10. Else
11. Else
12. $Node_i.Valid == false$
13. Delete($Node_i$)
14. End
15. End
16. End
17. End
18.
}

Simulation and Result:

Some of the parameters are much important to make and run any simulation in network simulator-2. The channel is a wireless channel, and the propagation model is radio propagation model and the MAC rule is following IEEE-802_11 protocol and communication is through two ray ground method communication. Also the other parameter settings are given in the following Table-2.

Table 2: Simulation Settings.

Parameters	Value
Network Size	1500 x 1500
Number of Nodes Deployed	10, 20, 30, 40 and 50
Routing Protocol	AODV
Sensing Region	50m
Total Simulation Time	50 ms

Our simulation is conducted within the Network Simulator (NS) 2.34 environment on a platform with GCC 4.3 and Redhat Linux. TAEACK is simulated on a laptop with core i^5CPU and 8-GB RAM.

RESULTS AND DISCUSSION

The algorithm defined in this paper is implemented using TCL language in NS2 and the results are investigated. Initially in the network there are 15 numbers of nodes are deployed and Sinkhole attack is simulated and verify the quality of the network in terms of throughput, delay, and energy, data loss.

The nodes are placed randomly in the network and it is depicted clearly in Figure-4. During the simulation, Node-13 try to communicate with the Node—4 by changing its ID as Node-8. The time, location, key and the original distance are verified from the Node-13 and it detected as Sinkhole node in the network and it is shown in Figure-4.

In order to measure and compare the performances of TAEACK approach we prolong to approve the following two performance metrics.

PDR: It means the ratio of number of packets received by the destination node which is sent by the source node.

RO: It means the ratio of the amount of routing - related transmissions.

$[RouteREQuest(RREQ), RouteREPly\ (RREP), RouteERRor\ (RERR), ACK, S-ACK, andMRA]$.

In the simulation S node broadcasts a REQ message to the neighbor nodes within its communication span. Upon receiving REQ message, each neighbor attaches their information with message and broadcast to the next level neighbors. In case of receiving the same REQ message twice it ignores. The failure node cannot detect the same message so that DSR sends RERR message to source node. It is so called routing overhead and it is shown in Figure-6.

To evaluate the performance of the TAEACK in terms of energy the remaining energy of each node is computed. The numbers of nodes are changed in each round and the remaining energy is computed using Equation-[1] and compared before deploying the TAEACK and after deploying the TAEACK approach. For all the rounds the energy is gradually reduced and the remaining energy is more in after deploying the TAEACK approach and depicted in Figure-7.

The throughput of the simulation result is obtained by executing an awk script for the trace file of the simulation output. The throughput is increased according to the number of nodes. Since throughput is high the packet loss is very less. In each round the throughput is getting increased and shown in Figure-8.

The delay taken to transmit the data packet in TAEACK is comparatively less than the existing approaches. The Figure-9 shows the delay taken by the network after and before deploying the TAEACK approach. It shows that the TAEACK takes very less time and hence it is efficient.

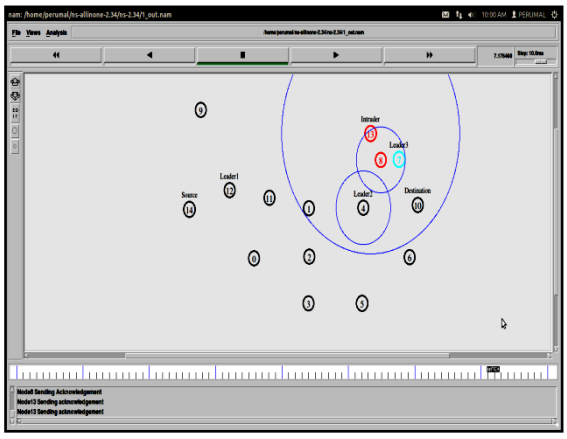

Fig. 4: Sinkhole Activity in NS2.

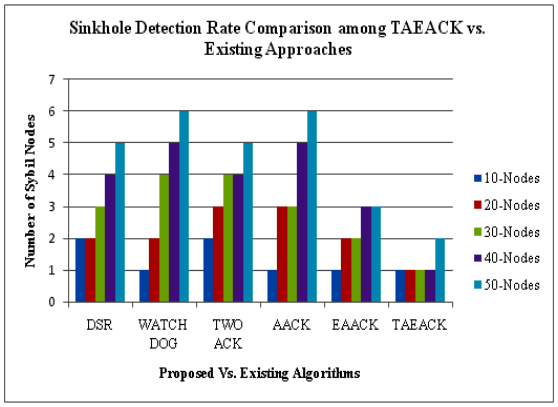

Fig. 5: Sinkhole Node Detection Rate Comparison.

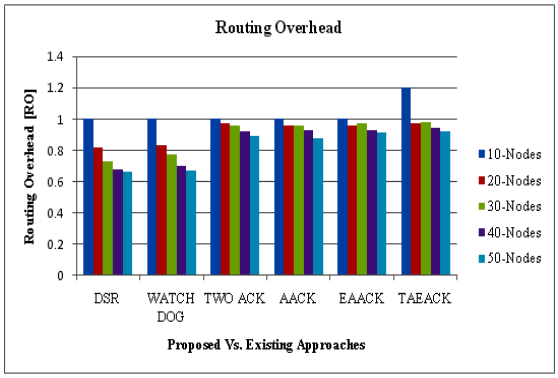

Fig. 6: Routing Overhead Comparison.

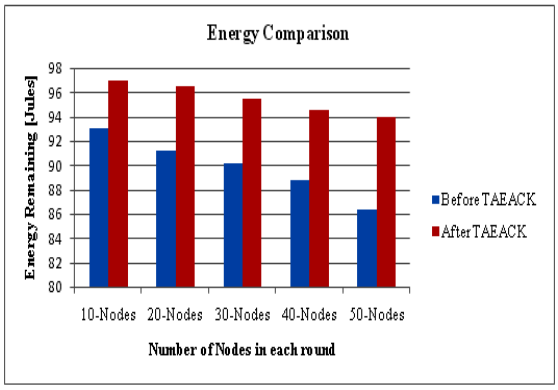

Fig. 7: Energy Comparison.

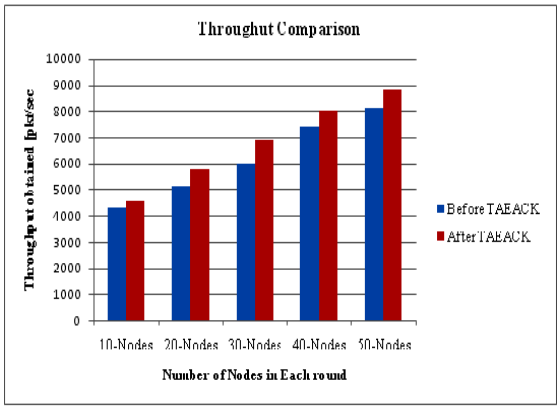

Fig. 8: Throughput Comparison.

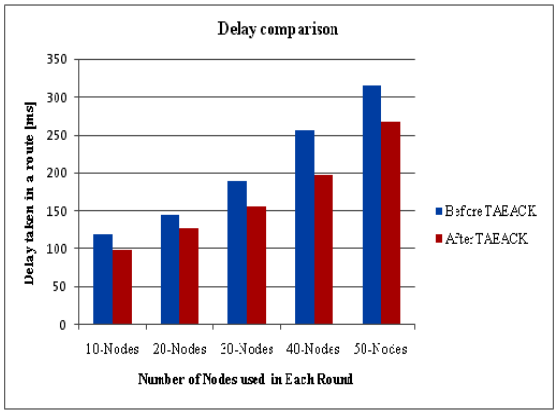

Fig. 9: Delay Comparison.

Conclusion:

In this paper we propose TAEACK approach for detecting and preventing Sinkhole nodes in mobility based MANET. We develop a comprehensive approach under DSR protocol where this approach is enabling for effectively detecting and preventing the sinkhole nodes without affecting the perpetual operation of the network. TAEACK provides good result in detecting malicious nodes and it provides prevention also. The efficiency of the TAEACK approach is making QOS of the network better in terms of malicious detection rate, throughput, delay and energy. The extensive simulation results demonstrate the efficiency and effectiveness of TAEACK, and the close match of energy neutral analysis with simulation results.

REFERENCES

Aboba, B. and D. Simon, 1999. PPP EAP TLS Authentication protocol. RFC2716.

Andre G´unther, Christian Hoen, 2004. "Measuring Round Trip Timesto Determine the Distance between WLAN Nodes", TKN Technical Reports Series, Berlin, 18.

Blunk, L. and J. Vollbrecht, 1998. PPP Extensible Authentication Protocol (EAP). RFC 2284.

Dhenakaran, S.S., A. Parvathavarthini, 2013. "An Overview of Routing Protocols in Mobile Ad-Hoc Network", International Journal of Advanced Research in Computer Science and Software Engineering, 3(2).

IEEE. 802.11i – IEEE standard for information technology – telecommunications and information exchange between systems - local and metropolitan area networks – specific requirements, part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, amendment 6: medium access control (MAC) security enhancements. IEEE Standards Board, July 2004.

Isha V. Hatware, Atul B. Kathole, 2012. Detection of Misbehaving Nodes in Ad Hoc Routing. IJETAE - ISSN 2250-2459, 2(2).

I-Wei Lai, Chia-Han Lee, Kwang-Cheng Chen, 2013. "A Virtual MIMO Path-Time Code for Cognitive Ad Hoc Networks", IEEE Communications Letters, 17(1).

Javad Pashaei Barbinand, Mohammad Masdari, 2013. "Enhancing Name Resolution Security in Mobile Ad Hoc Networks", International Journal of Advanced Science and Technology, 50.

Johnsi, J., G. Abija, 2013. "Reliable Data Delivery for Highly Dynamic Mobile Ad Hoc Networks Using Opr", International Journal of Emerging Technology and Advanced Engineering, 3(1).

Junliang Liu1, Zheng Yang1 and Ivan Stojmenovic, 2013. "Receiver Consensus: On-Time Warning Delivery for Vehicular Ad-Hoc Networks", IEEE Transactions On Emerging Topics In Computing.

Kartik Pandit, Dipak Ghosal, H. Michael Zhang and Chen-Nee Chuah, 2013. Adaptive Traffic Signal Control With Vehicular Ad hoc Networks. Ieee Transactions On Vehicular Technology.

Krishna K. Pandey, NiteshBaghel, Sitesh K. Sinha, 2013. "Optimum Relay Selection for Energy-Efficient Cooperative Ad Hoc Networks", International Journal of Modern Engineering Research (IJMER), 3(2): 1082-1087.

Muthumanickam, Kandhasamy, 2013. "SPAWN: a secure privacy-preserving architecture in wireless mobile ad hoc networks", EURASIP Journal on Wireless Communications and Networking, 2013: 220.

Pietro Michiardi and Refik Molva, 2001. "Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks.

Renato M. de Moraes, Hyunchul Kim, Hamid R. Sadjadpour, J.J. Garcia-Luna-Aceves, 2013. "A new distributed cooperative MIMO scheme for mobile ad hoc Networks", Information Sciences, 232: 88-103.

Rene L. Cruz, 2013. "Ad-Hoc Networks At Global Scale", International Conference On Computing, Networking And Communications (ICNC).

Rigney, C., S. Willens, A. Rubens and W. Simpson, 2000. "Remote Authentication Dial in User Services (RADIUS)", RFC 2865.

Saif Al-Sultan, N., Moath M. Al-Doori, Ali H. Al-Bayatti, Hussien Zedan. A comprehensive survey on vehicular Ad Hoc network. Journal of Network and Computer Applications.

Sasikala, G., L. Rajalakshmi, 2013. "Optimizing Bandwidth Utilization in Mobile Ad hoc Network", International Journal of Emerging Research in Management &Technology.

Sergio Marti, T.J. Giuli, Kevin Lai and Mary Baker, 2000. "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", ACM.

Stanley, D., J. Walker and B. Aboba, 2005. "Extensible Authentication Protocol (EAP) method requirements for Wireless LANs", RFC 4017.