CHAPTER 4

TAEACK: A TIME ADAPTIVE ENHANCED ACK MECHANISM FOR DETECTING AND PREVENTING SINK-HOLE ATTACKS IN MANET

4.1 Networking Aspects in MANET

Computer networking merits and demerits are understood by many sectors of today's rapidly increasing network topologies. Networks create temporary or fixed connections. The fixed connections are called as wired connection that is made up of cables; Temporary connection is the second one that is made of modems. In recent years, communication network includes wireless ad-hoc networks that play a major role. As devices connect, local area network (LAN) which is known to be ad-hoc network that built spontaneously. One type of ad-hoc networks includes MANET which has no infrastructure for its network that is no fixed or base station infrastructure is required for this method. During the run time of MANET, it can configure itself or change its location. This technique used as Wi-Fi connection or another medium that could be standard like satellite or cellular transmission. Both application and user traffic is generated by the nodes present in the network and carry out routing protocol and network control. MANETs advantages includes, cost-effective, self-configurable, consumes less time and more robust, rapid deployable and mobility.

4.1.1 Attacks in MANET

Active and passive are the two types of classification present in MANETs attack. The data which being transmitted through the network is attempted to modify by the attacker is known as active attack. The information from the network is gathered generally by the attacker is known as passive attack. Other attacks are commonly known as, Byzantine attack, wormhole attack, black hole attack, flooding attack, resource consumption attack and sinkhole attack etc.

4.1.2 Sinkhole Attack

Jeba Veera Singh Jebadurai et. al. (2011) Mobile ad-hoc networks facing a problem with sinkhole attack that is very dangerous attacks. For collecting the data from the network, sinkhole attack used compromised node that attracts all the traffic from the neighboring nodes by pertaining that it has the shortest path for the base station. Some discussion of related works is noted and various security challenges and issues are given in several papers which are discussed.

4.2 Background Study

Secure name resolution used for obtaining secured data binding with the people in (Javad Pashaei Barinand, 2013). For improving name resolution security, an identification scheme used by an earlier design and the system names are independent even it is offline or link failure. Petal routing protocol is proposed with efficient position-based opportunities in (J. Johnsi, G. Abija, 2013), the stateless property of geographic routing is used and for nodes mobility, wireless medium is used which I broadcast in nature. A control problem with energy efficient topology is proposed in (K. Krishna, Pandey, 2013) for co-operative communication that in CC network it uses optimum relay nodes are selected.

The energy consumption is reduced in the network. (I-Wei Lai, 2013) proposed a method of two coding schemes for virtual MIMO scenario. Here, end-to-end communication is enhanced, the path delivery exploited for its reliability. (Saif Al-Sultan) Discussed a VANET architecture and corresponding applications are relevant protocols. Separate vehicles of position information with data collection and aggregation based real-time speed that introduced by the same VANET. Also, (Kartik Pandit, 2013) proposed a method with help of OJF and OAF algorithms that optimize the signal for controlling traffic intersections.

(Rene L. Cruz, 2013) proposed a method for message forwarding using decentralized algorithm, and the message transmission occur using novel message format that considered by the author. For MANET, some routing protocols are proposed that helps for choosing appropriate routing protocol for different networks according to their conditions. (S. S. Dhenakaran and Parvatharthini 2013) paper provides comparative study by discussing various protocols. A secure privacy-preserving approach is used for securing genuine nodes in the network that proposed by (Muthumanickam and Kandhasamy, 2013).

For secure communication, the confidentiality is proven when node communicates with other nodes. In a network, the better solution for finding the ASWP problem is to apply k-shortest path algorithm and BFD [Bellman-Ford-Distributed] algorithm (G. Sasikala, L. Rajalakshmi, 2013). For improving delay, bandwidth and throughput in the network are achieved by utilizing TDMA scheduling to provide QoS.

(Renato M. de Moraes, 2013) introduce a new communication scheme with cooperative based MIMO-MANET, where end users are connected with M antennas that present in the network. Strategies discussed in (Junliang Liul, 2013) are an agreement of forwarding to achieve autonomously by the nodes under receiver consensus. (Pietro Michiardi and Refik Molva, 2001) discussed detail security issues present in mobile ad-hoc networks and performance that affect by relevant threats under DSR protocol.

(Sergio Marti, 2000) proposed a method that for eliminating or avoiding malicious nodes in the network with path rater provided by watchdog based security. Cooperative- IDS, watchdog, and path-rater are the various IDS used for detecting activities of the malicious node that explained in (Isha V. Hatware, 2012). Amalgamation is allowed for roaming endorsement methods by recent safekeeping standard 802.11i that based on other testimonials or public-key certificates. Blunk et al. proposed an EAP to apply with PPP protocol. In Aboba et al. discussed a method for EAP using TLS expansion. Rigney et al. (2012) form the RADIUS standard and enlargement as EAP. Stanley et al. proposed EAP methods and describe its necessities used in IEEE 802.11 wireless LAN in (B. Aboba and D. Simon, 1999). TAEACK method is proposed to overcome the wastage of memory and number of keys and better performance shown by the simulation result in security.

4.3 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.

4.4 System Model

The overall system model simulated for TAEACK is shown in figure 4.1. It shows the source node, destination node and the intermediate nodes in a route for data transmission.

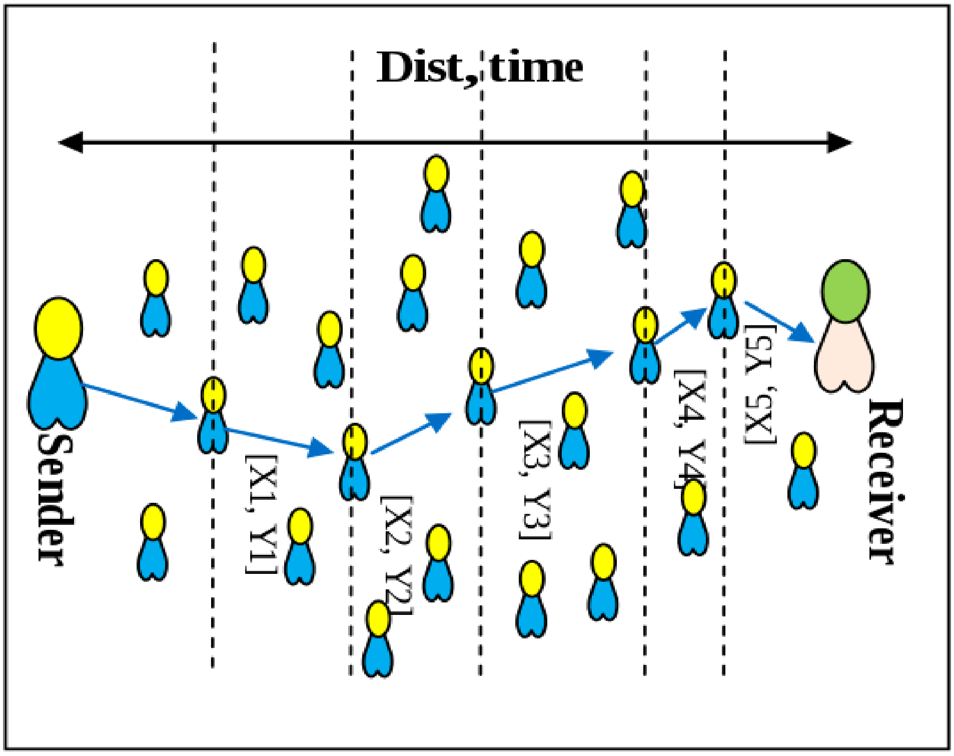

Figure 4.1 Proposed System Model

4.5 Proposed Approach

REQ-TIME is the request time and RES-TIME is the rest time that both mainly concentrated by this TAEACK model and by using the location of each node in the route for computing distance. ALWadHA approach helps to compare and estimate the location of nodes with computed distance. Euclidean formula is applied in this process and confirms the original distance between nodes and location of each node.

4.6 Network Model

Network M consist of N number of nodes. The data packets are transmitted by source node T to the destination node Q. Where$\{s_i, s_{i+1}, \dots \dots \dots \dots, s_N\}$, the route between T to Q has N number of nodes. The construction of route is carried out before transmission of data to Q by investigating entire nodes on the route from T to Q. The shape of the network area is imagined by rectangular, and column wise is depicted for entire network that divided into sub-regions as shown in figure 4.2, and source to destination node is treated as levels.

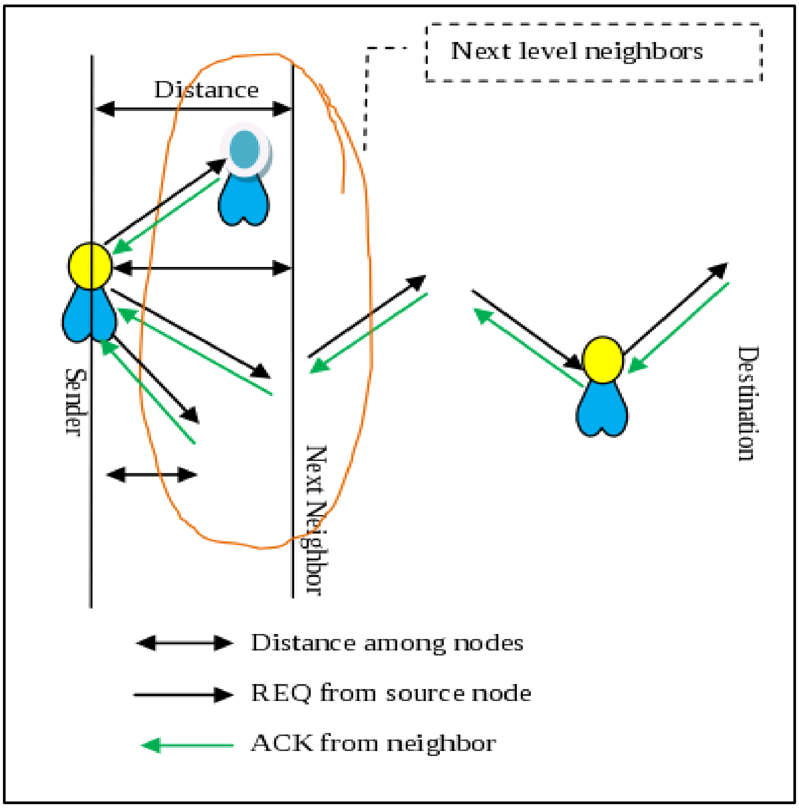

Figure 4.2 Neighborhood Management of Route Discovery

Many nodes are consisting in a network of each level and RREQ packet sent by source node initially to the next hop from its position ACK message is received. ACK receiving time and sending time of each packet are calculated. The calculation of approximate distance also processed and next neighbor node is assumed by its capability that which node takes less ACK time.

Next level nodes will get REQ, and an ACK is received from all the nodes that are available in them. TTL, location and node ID also provided with the ACK message. The fast reply is chosen by computing distances and ACK time and next neighbor node would be a less distance-based node that marked in the table. Local mode time and bandwidth are obtained by the distance among the nodes. The corresponding equation - 1 using remote node time is given below,

$$distance = \frac{[speed \times t_{remote} - speed \times t_{local}]}{2} \frac{T}{Q} \quad equation - (6)$$

Where,

Distance – is the distance between nodes

$\mathrm{t_{local}} -$ source node time [T]

$\mathrm{t_{remote}}$ – remote node time [Q]

speed – data transmission bandwidth

Calculation of neighbor node location according to the distance using,

$$[a_{remote}, b_{remote}] = [x - a_{local}, x - b_{local}] \quad equation - (7)$$

R_{table} is used for future reference that stores calculations of location and distance. It is processed ALWadHA approach for comparing estimated location with other. ALWadHA algorithm used for nearest neighbor method estimation by a location of the neighbor node.

This algorithm taken as a reference set for the set of nodes, that is already predefined the location of reference set or it used as Beacon node which it is initiated. The accuracy of location estimation is increased by the nearest reference method.

This approach is easiest and well defined nearest reference approach; the position of each node is computed by choosing a set of nearest neighbors. 3 beacon nodes are selected for computing neighbor node position with APS computation method also known as triangulation method. ALWadHA approach is also used for finding the location reference that provided by the attacker that is correct or not.

Table 4.1 R_{TABLE}

Seq.No	Node-Id	Location	Duration	Node-Key
1	2	120, 140	5 sec	Uu
2	6	130, 160	4 sec	Uu
3	7	210, 170	7 sec	9
:	:	:	:	:
N	I	A,B	D sec	Uu

There are four stages for completing functionality of the proposed approach given as,

- Node Registration
- Data Routing
- Route Discovery
- Cross Verification by Location Estimation

An ID is assigned for all nodes in the network [starting from single digit number] and A, B is the birth place of the location. A single node or source that named as T and assumed for first level nodes present in the entire network and number of node denoted N in the next level. REQ message is sent by node T at the initial process to all the nodes by next level and separately RES message received from those nodes and by using TTL, receiving time and message sending time is computed. For updating the information to routing table it chooses next nearest neighbor with REQ-RES time. Until destination node is not reached, the above process for finding the route of next neighbors is repeated and the routing table is updated with information regarding the nodes [ID, TTL, and Location].

R_{TABLE} is updated with route discovery when an entire node is available in the route and a key generated to provide more security. The route information has all nodes availability when data transmission occurs, and in terms of ID, A, B and TTL values the nodes are verified for validation. Dynamically, each node in the route generates a key, an equation -3 given for obtaining route discovery.

$$Key\ [Node_i] = append[NODE_{ID}, hopcount] \qquad equation - (8)$$

For example:

Key [Node-6] = append [6, 2] = 8 is the key for given Node-6.

In the route, one of the intermediate hop is Node-6. From the route, node-6 referred as 2nd hop node. The key of a node is given by node-6 is 6+2=8. R_{TABLE} is updated with intermediate nodes in which node security key is assigned and generated in the same way.

By providing TTL, location, and Node-ID to next hop that from R_{TABLE}, the information of node cross-verified when data transmission takes place. Once completing successful route discovery process, in the routing table, data packets are sent through nodes by source node ‘T’, once again, their information compared and pass the data in the routing table. If the information submitted by the node is not matched with information in the routing table, then, the node will be assigned to malicious and eliminate the node from the network and broadcast the information about this malicious act of the node to all other nodes to avail further security in the network.

Packet size is → v

Number of the packet is → vn

t_0 → node0 to node1 packet delivery time

t_1 → node1 from node0 packet received time

Then $t=t_0 - t_1$ and distance among the node is $d = v * vn/t$.

The nodes location not correctly submitted by the malicious node or reference node when computed distance is not accurate, and not all the information provided correctly and mainly the location. ALWadHA is the Location Estimation Algorithm that computes the location of the node correctly and accurately estimated for suspending nodes.

4.7 Location Estimation

For computing and estimating the location of nodes, a special node is assumed from some of the nodes and named as beacons that are used for location discovery. With the help of manual configuration or GPS receiver, beacon nodes acquire the locations. The location of the remaining nodes can be computed with the help of beacons and the location is currently known as unknowns.

In the networks, some nodes are trustable node as same as trusted beacon nodes as given in this paper. Since beacon nodes know their location by itself and while transmitting messages, their location is broadcasted to other nodes. At beginning stage, itself, the location of all nodes accurately computed using characteristics of beacon nodes. Node submitting locations are compared whenever it needed, also verified by using the location of beacon node.

Transmitting a data packet, receiving a data packet, sleep, idle and listening are the various states that help to wake up energy in a different amount that reduced from nodes initial energy. The initialization of initial energy is given by 100 joules. Some amount of energy for each state is assigned and predefined.

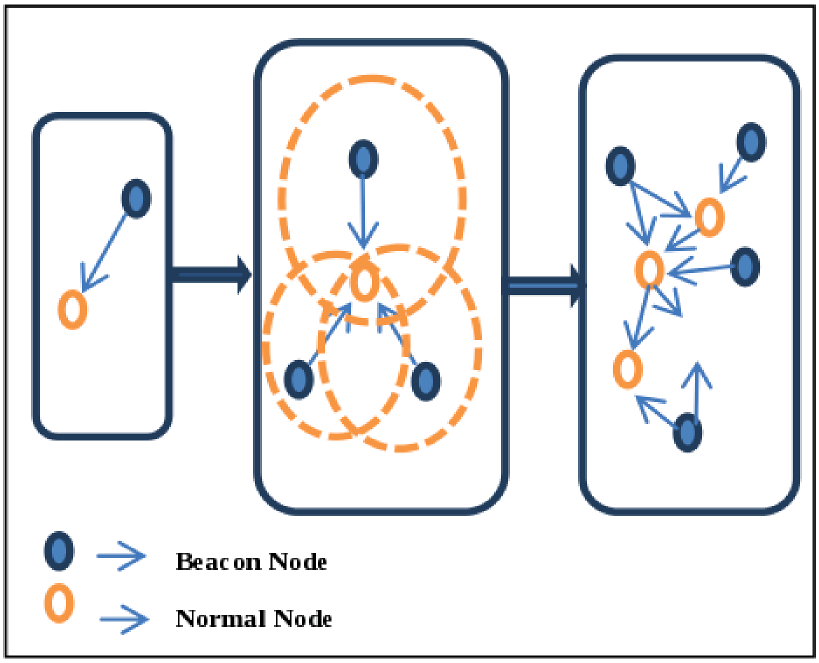

Figure 4.3 ALWadHA Model for the Localization system

Energy initially given = 100 Joules

Energy Transmitting = 0.26 Joules

Energy Receiving = 0.08 Joules

Idle Energy = 0.01 Joules

Energy for Sleep = 0.005 Joules

Energy for Wakeup = 0.005 Joules

A formula is used for updating initial energy in each round and is given as,

$Initial\_Energy$ = [Receiving Energy + Sleep Energy + Transmitting Energy + Listening Energy + Idle Energy + Wakeup Energy]

Algorithm TAEACK ()

```
Step 1:  Network M ={$k_1, k_2, k_3 \ldots \ldots \ldots .. k_N$}, BS is the base station
Step 2:  For I = 1 to N
Step 3:  Key ($N_i$) = append [Node-ID, hop count]
Step 4:  END
Step 5:  For J = source to destination
Step 6:  If (Key [$Node_i$] = = Key – table – row[i]) then
Step 7:  If (Node-ID.exist ($R_{TABLE}$) then
Step 8:  If (Node-A, Node-B.exist ($R_{TABLE}$) then
Step 9:  data ($Node_{i+1}$) = data ($Node_i$)
Step 10: Else
Step 11:    Else
Step 12:      Else
Step 13:         $Node_i$ . Valid = = false
Step 14:          Delete ($Node_i$)
Step 15:      End
Step 16:   End
Step 17: End
```

4.8 Simulation

To run or make a simulation in Network Simulator – 2, some parameters are more important. Wireless channel is used for this channel and radio propagation model is the mainly used for propagation model. IEEE 802.11 protocol is followed by MAC rule; two-way ground method is used for communication. Table 4.2 shows the other parameter settings.

Table 4.2 Simulation Settings

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

Network Simulator (NS) 2.34 environments have used for conducting simulation for the work and GCC 3.4 used as platform and Redhat Linux as operating system. The system configuration is core i^5 CPU and 8-GB RAM for simulation of TAEACK.

4.9 Summary

The TAEACK approaches have been used for the detection of sinkhole attacks as well as prevention that mobility based mobile ad-hoc networks. Under DSR protocol, a comprehensive approach was proposed to enable detection and prevention of sinkhole nodes in the network without affecting the effective operation. The proposed approach TAEACK gives better results for detecting malicious nodes in the network. QoS of the network becomes better in terms of throughput, energy, malicious detection rate and delay. The effectiveness and efficiency of TAEACK was demonstrated by the simulated results and energy neutral is close match with the result of the simulation.