I J C T A, 10(20), 2017, pp. 207-220 ISSN: 0974-5572

Connection Termination Period Based Secure Warmhole Detection Scheme in Manet

Vijitha S.* and Bhavani**

ABSTRACT

The mobile ad hoc networks are widely employed in various applications. The network is composed of dynamic nodes communicating with one another and it does not require any central administrator. Due to the presence of dynamic nodes the network is vulnerable to several types of attacks like active or passive attacks. These attacks can corrupt the performance of the entire network, i.e. network connectivity, availability of the network and the coverage area for transmission. Secure wormhole detection scheme (SWDS) is proposed which is based on Connection Termination Period (CTP) inorder to survive the wormhole attacks . This technique is implemented to find the wormhole attacks to equalize the protection among the route and steadiness between the connections. In addition, the scheme uses the Updated Twofish scheme for encryption and decryption of network information in order to protect it from the wormhole attackers. This scheme provides one half as normal encryption and next half as modified encryption for communication from sender node to target node. The results of simulation reveal that the proposed scheme attains better throughput, enhanced packet delivery ratio, minimized overhead and packet losses as compared to the conventional TETC, FTD and PCR schemes.

Keywords: Index terms-Mobile Ad Hoc Networks, Vulnerable, Wormhole, Connection Termination Period, Connection Steadiness.

1. INTRODUCTION

The mobile ad hoc network is a self organizing network without any fixed infrastructure. The nodes present within this network has a capability to act both as host and router at the same time. i.e. the nodes need to join during forwarding data to other nodes and makes quick decisions regarding the next node that need to forward data packets depending on the connectivity of network. The mobile ad hoc networks serve many applications like military networks, emergency operations during floods, hurricane or earthquakes and it is not necessary that all applications run on a trusted authenticated environment for which security must be ensured [1]. But due to the open nature and infrastructureless design these networks are vulnerable to several security attacks. The various injuries threaten the security in wireless networks and creates differences within the network troubling the upper layer applications. For black hole attack,the malicious node advertises fake routing path and shortest route to destination , subsequently leading to dropping of data packets in nodes within the receiving time[2]. Black hole and wormhole effects are risky as compared to other type of attacks because the attacker is capable of creating other types of intruders like a packet dropping, replay attacks, eavesdropping, flodding attacks. In flooding ,attack causes packet loss, end to end delay is increased, packet transmission is mostly among attackers present the in network environment [3].

During communication a worm hole attacker node detains packet from one location within the network and passes them to another malicious node present at a larger distance. The detaining can be performed either as in band or out of band which makes the detained packets to arrive either sooner or with only less

* Research Scholar Karpagam University of Engineering and Technology.

** Professor and Head Karpagam University of Engineering and Technology, Coimbatore, India.

hops as compared to the packets transmitted over the normal multi hop routes [4]. This creates a delusion that the end points appear closer to one another, but they are actually not because this delusion is created by the malicious node to degrade the performance of the network.

2. RELATED WORK

The contributions of various scholars are studied for analyzing the merits and demerits in order to enhance the learned drawbacks for making the system work better. Darshana Sorathiya et.al [5] presents mobile nework performs less communications among mobile nodes in which nodes move around the network with different direction randomly. Nodes normally communicate by transmitting the information to neighbour nodes available in network. During packet transmission attacker tries to interrupt network, various types of attacks are available in network environment. Present method evaluates to identify and avoid wormhole attack and compares them. Mobile networks have a large area in which safety is a main issue. Variety of attacks and protocols that humiliate the performance of the network, have different methods to find and remove attacks. This technique includes extra packet known as hound packet. Hardware is not consider to finding attacks in network.

Badran Awad et al, [6] presents an innovative model for detection and prevention of wormhole attacks based on hop-count metric called BT-WAP. In BT-WAP effectively and professionally isolates both wormhole node and colluding node. It also monitors the node history for every packet transmission and it uses minimum energy for each transmission. The BT-WAP method removes the attacker node present in network. Acceptable detection rate and detection accuracy rate is enhanced by the application of BT-WAP in network environment. Those kind of intruder generates network issues and corrupts the entire network. Also it launches authentication problem and confidentiality problems. Misbehaving nodes distrupt packet transmission in network. Proposed an effective model for finding and removing wormhole attacks. In the direction of finding wormhole tunnels,it uses hop-count metric inherited from routing protocol, BTWAP model is simple method to deploy and moreover it notrequire the use of hardware equipments. Simulation result of BT-WAP techniques indicates an enhanced detection rate under different scheme. It also contains a encryption algorithm, to enhance security, and minimize energy consumption.

Prerna Priyadarshini et al [7], proposed some successful techniques in MANET Research area. In MANETs nodes are motivated frequently, and have no fixed position, self-governing network have many protection issues to minimize the network performance. Proposed a scheme called Reference Point group model to detect worm hole attacks and successfully compared with the Two Ray Model.This method detects wormhole attack by measuring the distance of nodes which were present in path and done its prevention by changing the paths when wormhole attack is detected, compared results using metrics :- throughput, energy and delay which shows that reference point group model uses less energy, less delay and better throughput than random way point model. It is designed for more dependable and well-organized network with the confirmation that the attacker is not able to distrupt the network another time in outlook by trust analyze history of each nodes in network.

Muhammad Imrana et.al [8], proposes Wormhole attack as one of the most severe routing attacks made on communication networks, which is simple to deploy but difficult to detect . Usually, operates in two steps: first the wormhole nodes creates a channel and absorbs all the traffic towards it though the channel and in the next step attacker tries to change the information in packet causing changes in network traffic.. Diferent features like location,time,hopcount of different methods especially Intrusion Detection Systems are analysed . It designs an efficient IDS to find wormhole attacks in mobile network. The methods based on route request (RREQ) or hop add up gives better results than other methods to find wormhole attacks.

Neha Dubey et.al [9], proposes a secure and efficient approach for the detection of the wormhole attack in the Mobile Ad Hoc Networks. The algorithm is implemented on a very popular on Adhoc On Demand

Distance Vector known as AODV routing protocol. The beauty of this proposed algorithm is that it not only identifies the wormhole attacker node but also confirms it as well.This method reduces processing delay and improves speed of searching.The protocol is invoked only when a node (host) has data to transmit. It is a reactive protocol. The AODV RFC indicates that the transport layer protocol is UDP, which of course only offers best effort delivery of packets, and does not support either error recovery or flow control.

S. Nivedha et al, [10], identifies importance of protection in mobile adhoc network. One malicious node receives packets from one location, tunnels them to a different malicious node situated in another location of the network and disturbs the full routing technology.. All routes are so directed to the wormhole established by the attackers. The entire MANET system would be victimizedby the worm hole attack. It surveyes many existing ways to notice wormhole attack in mobile adhoc networks and proposes a new fresh wormhole detection and prevention algorithm that will effectively notice the worm hole attack in mobile adhoc network. Aims to enhance packet delivery ratio amidst the worm hole attack and also reduces the overall packet overhead with an upperhand on security. It also improved the detection ratio with higher security in Mobile ad hoc network.

Neha Sahu et.al [11], proposes a dynamic wormhole detection and prevention technique AODVWWP which is based on an hybrid model that encapsulate location ,neighbour node and hop count method. A MANET faces a lot of security issues due to the nature of its deployment. AODVWWDP (AODV with wormhole detection and prevention) selects a wormhole free path from source to destination. A secure path is required to reach the destination the source broadcasts the packets which are taken by the neighnouring nodes and relayed till the destination.All the neighbor node follow up the request forwards and replay a route replay packet to source node, then source node select shortest and less traffic path for transmission but because of that greediness some time source node select wormhole effected path for transmission. AODVWWDP enhances the performance of AODV by adding one more rule over selection criteria ie select wormhole free route, it depends on hybrid model, covers the location of neighbour node and hop count method. Hybrid methodology to find wormholes and removal of the same in mobile ad hoc networks is suggested power consumption in network. In order to identify wormhole this method employs maximum count of control packets.

Chandandeep Kaur et al, [12] proposes secured communication over unreliable network for military application using mobile ad hoc network and also in urgent situation reply process like an overload, and time delay. Identifies wormhole attack by analyzing the distance between nodes that are available in path and by complete avoidance by modifying the channels while wormhole attack is identified. Analysis of performance on transmission rate, energy usage and end to end delay indicates that suggested Random point group method uses less energy, less end to end delay and better throughput than Random way point model.

Parul Singh et al, [13] presents latest secure routing protocol, ODSRP-LET-On-demand secure routing protocol based on LET also known as Transmission based link Expiration Time Channel (TETC), then it depends on LET-Link Expiration Time for source node transmitting packet to destination node in a network. Straight routing protocols like AODV, DSDV, and DSR, from time to time appearance untrustworthy link that breaks the connection. To renew failure connection, chanell processing activity creates efficient traffic control, link failure leads to packet get loss. It increases the security for data packet transmission through RSA algorithm –an asymmetric key cryptography that gives privacy. ODSRP-LET method improves in link dependability and minimizes the traffic, and enhances the privacy of data. Finally security and reliability of packet transmission is improved.

Jyoti et al, [14] present a survey on the formation of collective network and deformation on-the-fly lacking the need of any centralized management. In packet transmission, two way model and broadcast medium also support intruder to interrupt network environment. The importance of this survey is a check

on various wormhole attacks and use of few detection scheme and various methods to avoid network from these intruders. The type of detection and avoidance of wormhole depens mainly on the cost, need of protection o obtain efficient output, and to some extent the hardware also.

Yashpalsinh Gohil et al, [15]. Proposes a protocol to be implemented in the mobile Adhoc networks using AODV protocols. In this approach, a secret key is used to encrypt the data packets in the network. It means only authenticated node will get the request packet and can reply. In this way, the mechanism provides better throughput and less packet drop over the wormhole attack is influential so identification is not easy, it creates a lot of problems during communication.It emphasizes on position based security system.Design of effective hardware to improve security provides improved end result,but is of high cost, that influences other needs of networks

Nidhi Nigam et al, [16] addresses the wormhole attacking issues by introducing a new co-operative, relative approach, based on Reference Broadcast System (RBS). Proposes the concept of velocity between the sender and receiver nodes to improve network scalability and throughput.Three mechanisms proposed are AODV, threshold setting using RBS, and ACK for dependability of transmission, to detect wormhole attacks in ad hoc networks. It also discusses a semantic security mechanism to withstand attacks based upon packet dropping and message tampering. The known malicious nodes are isolated for future sessions in network.. This method is efficient and secured over hazards available in network.

Ziming Zhao et al [17], presents various types of attacks and their solutions as WSN are succeptible to vulnerable attacks. Previous results usually separates attacker nodes based on binary reply status and navie fuzzy reply status. However, binary reply cause report in the unpredicted network separation, arise extra loss to the network infrastructure, and naive fuzzy reply can guide to finalize removing processing attacks in Mobile network. It also presents a risk-aware response scheme to methodically manage detecting attacks in transmission time. Risk-aware method depends on an improved Dempster-Shafer numerical assumption of verification applied to analyze various parameters.

G. Santhi et al, [18] provides an efficient Quality of Service (QoS) for secured communication in networks. Quality of service plays a vital role in real time application. GPS-Global Positioning System is used to find the location of nodes , and choose the transmission path efficiently with RET-Route Expiration Time. Group of fixed and updated mobile nodes are used for transmitting data packet through the path. Result of simulation indicates that present protocol attains an efficient result such as enhanced packet delivery ratio and minimized end-to-end delay. Sender broadcast the data packets effectively to particular intermediate nodes with high speed and connection should failed for each packet transmission. Group of fixed and efficient mobile nodes are used to achieve route discovery and route security. Transmitting path satisfies numerous QoS constraints according to the QoS persevere. It reaches maximum packet delivery ratio and minimum end to-end delay as compared with MAODV.

ZHOU Yao et al, [19] Present at rest some flaws in PCR multiculster method. In present work follows short survey scheme and a innovative CNS algorithm with novel multicluster PCR scheme is introduced. Simulation report gives a better performance improvement with minimum complexity. It is very strong and valid one compared to previous PCR. A history of multicluster PCR scheme for major role in new CNS algorithm implementation, it obtain result have higher throughput, it not mention extract position information of node movement.

Lianghui Ding et al, [20] presents a method that uses storage buffer for each intermediate nodes and launch the structure for combined arrangement and choose intermediate nodes which leads to increase in network efficiency.Two JSRS-joint scheduling and relay selection algorithms for transmission/receiving data packets are analysed since any packet overload,cross-layer intermediate nodes' historical information is considered to select route in present algorithms. JSRS with buffering is improved compared with traditional FTD without buffering technique. Joint scheduling and relay selection algorithms for both single-way and dual-way intermediate networks

include history of cross-layer intermediate node choosen along with instantaneous channel conditions in a first in first out manner. Performance results confirm the throughput of JSRS is better than FTD . The output reports that buffer sizes only have a minimum control on the performance of JSRS method.

2.1. Problem Addressed

The wormhole attack is a severe attack which occurs during routing in MANET, where two attackers are linked together through a high speed off – link medium, but are positioned at different places within the network (fig.1). The attackers overhear the data transmitted through the wireless medium and routes them between one another and replays these packets to the other end of the network. The message replaying among the network at different places allows the worm hole attackers to make believe the far away nodes that they are the immediate neighbors and forces all communications to happen between these affected nodes to go through them. The wormhole attack is worse for all types of routing protocols in mobile ad hoc networks.

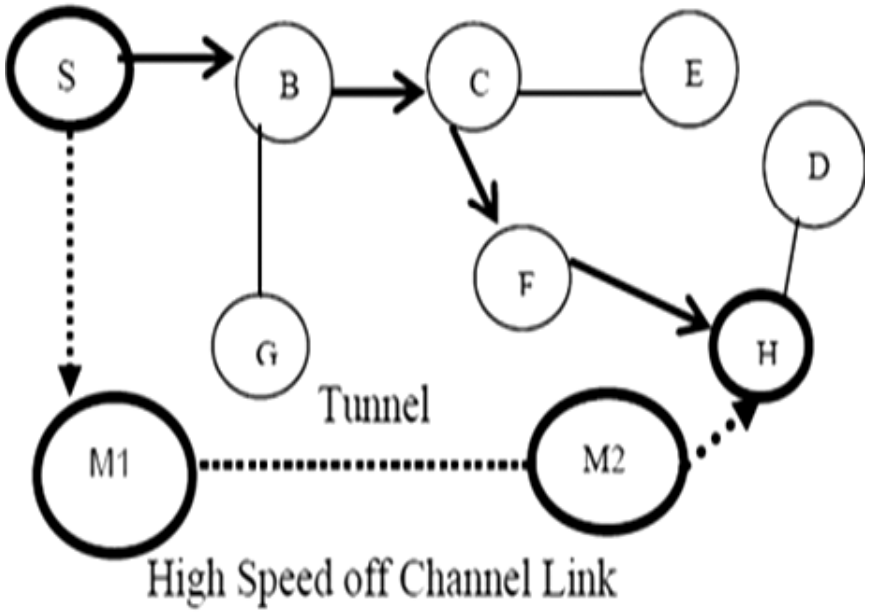

Figure 1: Wormhole Attack in MANET

3. PROPOSED METHODOLOGIES

Based on the investigations from the literature survey of various scholars the solution to the problem was achieved which are classified and presented below. The wormhole attack detection mechanism based on the Connection Termination Period (CTP) between the nodes is proposed with modifications. The proposed scheme allows the receiving node to accept a RREQ-route request or to send a RREP-route reply packet based on calculating the Connection Termination Period (CTP) of the node with respect to its sender. The connection Termination period predicts the time until two nodes remain in connection with one another. The data integrity and authenticity are provided using the Modified Twofish scheme.

3.1. Connection Termination Period (CTP)

The present method utilizes the information related to the location and speed information about the every individual node. Based on the mobility parameters are two closely organized nodes the time length by which the two nodes will keep on connection steadiness is calculated. It is considered that the two nodes x-axis and y-axis remains within the communication range of each other neighboring nodes.

For any two mobile nodes e and f, let (x_e, y_e), $(x_f, y_{f)}$ be the coordinates of mobility. Let and ve and vf denote the speed of mobile nodes e and f and the direction of moion is. described by d_e and $d_{f,}$ where, $d_e \geq$

0 and $d_f \leq 2\pi$. The quantity of time the two nodes e and f remains connected that is $CTP_{e\text{-}f}$ is calculated as below.

$$CTP_{e-f} = \frac{-(ef+gh)+\sqrt{(e^2+f^2)r^2-(ed-fg)^2}}{e^2+f^2} \quad (1)$$

Then, $e = v_e \cos d_e - v_f \cos d_f$, $f = x_e - x_f$, $g = v_e \sin d_e - v_f \sin d_f$ and $d = y_e - y_f$.

Sender node transmits request packets to single hop neighbor nodes. The Location and Mobility details of source node are stored in request packet for each transmission along with transmission rate and the connectivity as the packet contains the location, mobility, velocity information.

On the reception of request packets, the single hop neighbors calculate the CTP with respect to the source node and the routes to the source node are updated with all the information related to speed, location and velocity. This information is appended into the source node. i.e. after the reception of request packet the CTP is estimated with respect to the sender node. This request packet is forwarded throughout the network to obtain the path for data communication.

After the reception of request the destination side responds by creating a reply packet.The request from the source node is placed into the reply along with a $CTP_{s\text{-}r}$. The source route within the reply is multicast to the nodes such that each node on receiving the reply appends the CTP and it calculates the request reception time. After collecting all the reply from all the nodes by the source node the data packets are transmitted to the route which satisfies the following condition.

Sender node needs to transmit request packets to single hop neighbor nodes. Location and mobility of source node details are stored in request packet for each transmission. Furthermore, the transmission rate and the connectivity are also provided, because the packet contains the location, mobility, velocity information.

Upon receiving a request packet by single hop neighbors the calculation of CTP is performed with respect to the source node and the route to the source node is updated, all the information related to speed, location and velocity are appended into the source node. After the reception of request packet the CTP is estimated with respect to the sender node. By forwarding this request packet throughout the network the path for communication is obtained.

After the reception of request on the destination side the response is created as a reply. The request from the source node is placed into the reply along with a $CTP_{s\text{-}r}$. The source route within the reply is multicast to the nodes, so each node receiving the reply appends the CTP and it calculates the request reception time. After collecting all the reply from all the nodes by the source node the data packets are transmitted to the route which satisfies the following condition.

$$\text{Min}(CTP_{S\text{-}R}) \geq CTP_T \quad (2)$$

$$CTP_T = \frac{No.\ of\ Packets\ interacted}{No.\ of\ packets\ to\ be\ sent\ per\ seconds} \quad (3)$$

At this point, Minimum ($CTP_{s\text{-}r}$) is the lease value of CTP in the request packet ,and CTP_T is the amount of time the transmitting node requires to communicate the packets. Upon receiving more than one reply by the source node based on above function that particular route will be chosen because it contains only least CTP and the other possible routes will be stored. In case if all the obtained routes have least CTP then the routes are chosen by the node itself.

Algorithm for Route Prediction based on CTP

For each route

For each link

If(Min(CTP_{S-R})==CTP_T) //Send all packets through this route //after //sending packets no other //routes are checked

End If

End For

End For

If (no route is found)

Set Min_CTP= max_value // max_value is any //stable value greater than //all the CTPs of each route // already known

For each route

For each connection

If(Min (CTP_{S-R})>CTP_T)

If(Min_CTP> Min(CTP_{S-R}))

Min_CTP = Min(CTP_{S-R})

End If

End If

End For

End For

If(Min_CTP ‘‘‘max_value) //Send all packets through the route which has CTP value equal to Min_CTP

Else

No route found

End If

End If

3.2. Protection based Wormhole Detection using Updated Twofish Algorithm

The source node S communicates a message to the destination node D for creating a user key and password key to perform communication among nodes using UT-Updated Twofish algorithm. Source Node receives a reply message from the destination node D within the Connection Termination period (CTP). CTP should be maximum predictable time to wait to obtain a path reply PREP packet, after the transmission of path request PREQ. The source node and the destination node implement the UT algorithm using CTP method. The source S sends an encrypted message with a block mode BM to the destination using advanced encryption time and those information are stored in buffer. The destination D decrypts the BM information to AM-Active mode information. The encryption ID achieved using UT and communicates it back to the source node.

In case, if the source S does not receive the reply packet within the Connection Termination period (CTP) then the source S confirms that the path is affected by intruder node in the network. Detected attacker node route is eliminated from the entire network, but all these informations are maintained in the buffer. Always the single hop neighbor nodes are checked to analyse the routes to which they are connected . This information may be accepted on the next single hop neighbor else the time taken to receive the information and the details stored in the buffer will be estimated. Sender node determines the

unique time taken for broadcast that is the stipulated time taken for sending request until the request is received by neighor node.

When the total time $Time_{nk}$ is less than or equal to the connection termination period (CTP) it can be calculated based on fake node causing packet drop in each transmission. Request and reply time is estimated for total time $Time_{nk}$ as follows:

$$Time_{nk} = RS_t + RR_t \tag{4}$$

Where RS_t Request send time and RR_t Reply received time. If any packet loss ocurrs the maximum time required for retransmission to overcome this loss uses UT algorithm and checks the priority. Higher priority node causes the minimum packet loss whereas lesser priority node cause the maximum packet loss.

$$UT = Buf\,(constant\_data) + Time_{nk} \tag{5}$$

Where, *Buf*(*constant_data*) indicates the constant_data information maintained in buffer storage with total time taken to transmit packet and receive reply packet between neighbor nodes which route is efficient one are analyzed. It minimizes the packet drop rate and enhances the network lifetime for end to end transmission, UT supports the successful packet transmission, it also increases the network protection from any unwanted intruders.

This phase, utilizes both encryption and decryption schemes. There is no need for cipher text conversion, get the user name key and password key using that to encrypt the constant data packets into cipher-block chaining mode. All data packets are not still only on particular cipher type, that are updated. In receiver side to decrypt those kind of information use pwd and user keys. It improves the authentication among transmission between sender node to receiver node.

Encryption phase

1. Node=constant_data;
2. get(userkey [32]);
3. get(pwdkey [32]);
4. Bufferstorage inBuf [16], outBuf [16];
5. Memory_allocation (& twofish , 0 , sizeof(TWOFISH_CONSTANT_DATA));
6. allocate_key (& twofish.key , (DWORD*) userkey, pwdkey, 256);
7. UpdateTwofish_encrypt (&twofish.key, (DWORD *) inBuf, (DWORD*) outBuf);

Decryption phase

1. Update Twofish(constant_data);
2. Fix Stream mode(constant_data);
3. After some time slot fix Active mode(constant_data);
4. Fetch the data from various updated modes.
5. put(userkey [32]);
6. put(pwdkey [32]);
7. Deallocate_key(&twofish.key, (DWORD *) userkey, pwdkey, 256);.
8. UpdateTwofish_dencrypt (& twofish.key, (DWORD *) inBuf, (DWORD *) outBuf);

The following are the cryptographic primitives used in the stream mode, its like a block mode no need to change the content of data packets. In active mode data's are decrypted using the user key and password key.

1. Block mode, each digits of the information is encrypted independently.
2. Active mode constant data packets are ready to decrypt the information in normal form.
3. Some algorithms support both modes, others support only one mode. In the block mode, the cryptographic algorithm splits the input message into an array of small fixed-sized blocks and then encrypts or decrypts the blocks one by one.
4. The condition is varied through the encryption and decryption procedure and shared with the information of all sector. It reduces the issues with the same sectors and may also provide for extra activities.
5. Check the entered user key and password key with already buffer stored key, if match successfully decrypted else mismatch occurred for decryption key.

4. PERFORMANCE ANALYSIS

The proposed SWDS performance metrics are analyzed using the network simulation tool (NS 2.34) and compared with TETC [13], FTD [20], and PCR [19] schemes. For simulation purpose, 100 dynamic nodes

Table 1
Simulation Parameters

No. of Nodes	*200*
Area Size	1150 × 900
Mac	802.11
Radio Range	250m
Simulation Time	45ms
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Protocol	AODV
Pause time	5 ms

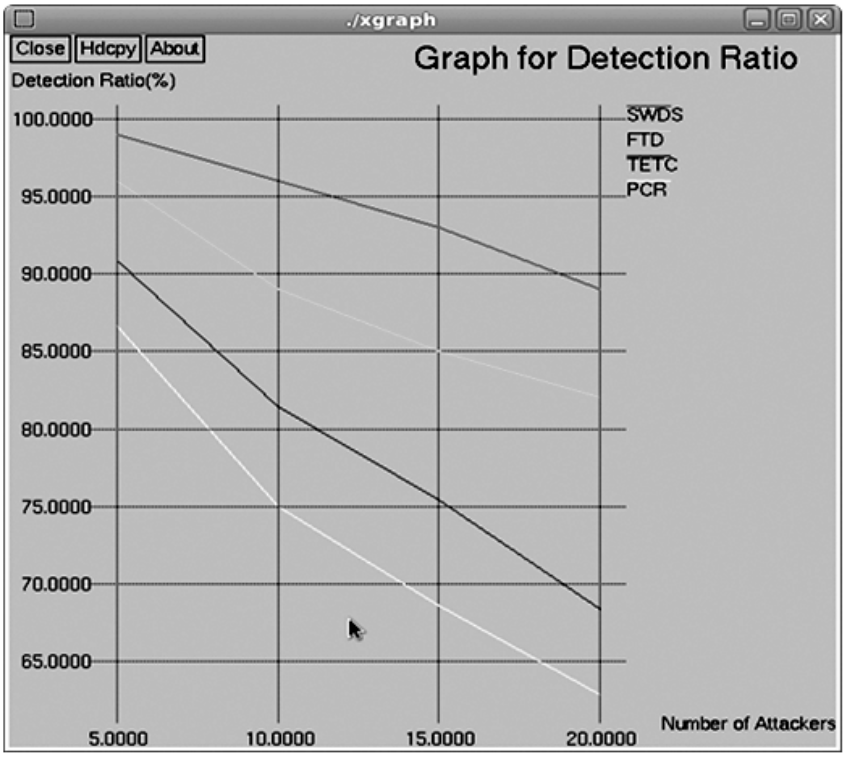

Figure 2: Attacker Detection Ratio

are made to move in 1150 × 900 meter square regions for about 45 ms. The transmission range of all the nodes is 250 m. The traffic considered for the simulation is constant bit rate (CBR) and Poisson traffic. The settings and parameters considered for the simulation are tabulated in Table [1].

The simulation results of Secure Warmhole Detection Scheme (SWDS) are compared with existing TETC, FTD and PCR in the presence of a congestion environment. From Fig [2] the ratio for attacker detection for varying ranges between 5 to 20 for the proposed SWDS scheme is performed which provides an improved attacker detection ratio based on the CTP as compared to the existing TETC, FTD and PCR schemes. From Fig [3] the results of the packet delivery delivery ratio can be perceived for varying mobility of up to 250 nodes and the node moves between 60 to 90 ms. It is clear that the proposed SWDS achieves a improved packet delivery ratio as compared to existing TETC, FTD and PCR schemes due to RSA.

From Fig [4] the overhead for the proposed SWDS can be viewed for nodes varying up to 250. The results depict that the proposed SWDS scheme achieves reduced overheads as compared with the existing TETC, FTD, and PCR schemes.

From Fig [5] the throughput for the proposed SWDS can be viewed for nodes varying up to 250. The results depict that the proposed SWDS scheme achieves increased throughput as compared with the existing TETC, FTD and PCR schemes.

From Fig [6] the average end to end delay is depicted for the proposed SWDS scheme which achieves reduced delay due to increased packet delivery ratio and reduced overhead for varying nodes of 250 for 30 ms as compared to the existing TETC, FTD and PCR schemes.

From Fig [7] the results of the packet loss can be perceived for varying mobility of up to 250 nodes between 4 to 35 ms. It is clear that the proposed SWDS achieves reduced packet losses as compared to existing TETC, FTD and PCR schemes due CTP based SWDS scheme.

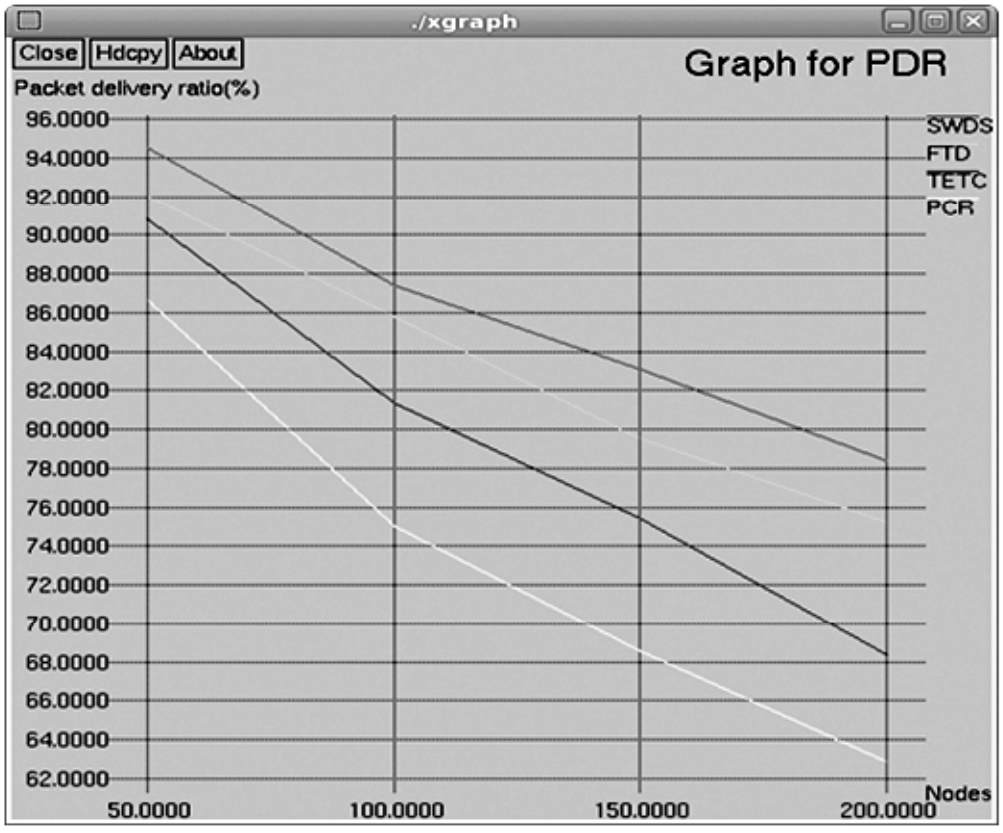

Figure 3: Average Packet Delivery Ratio

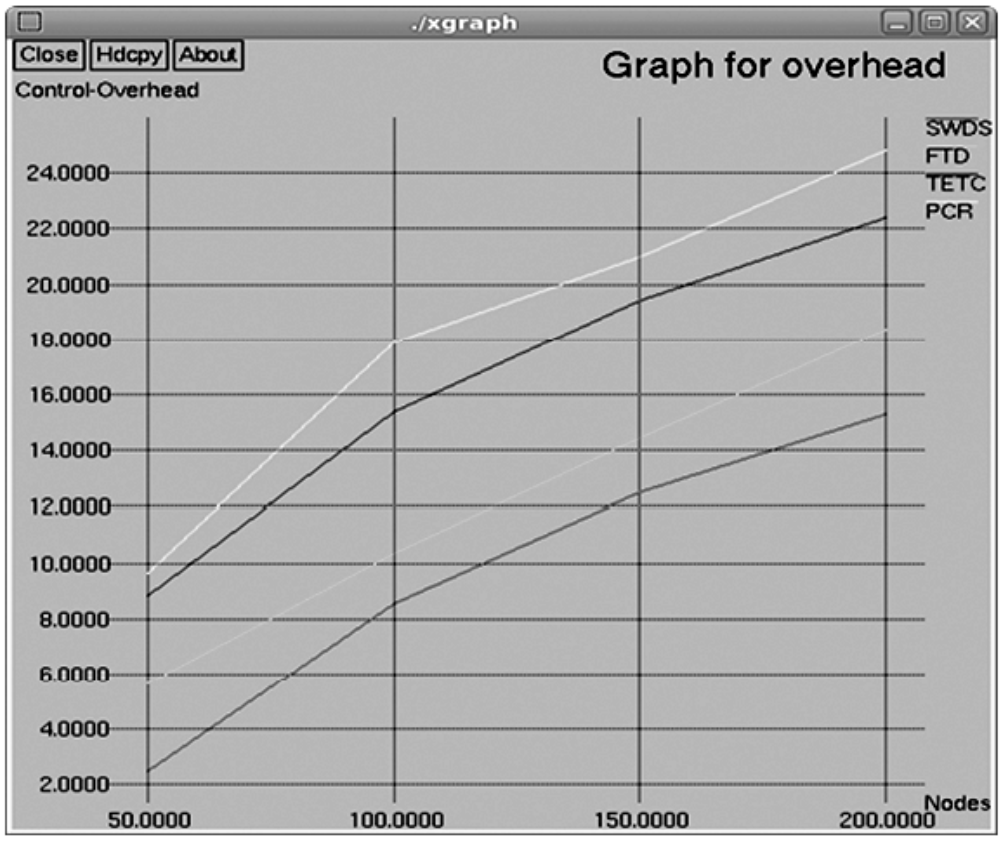

Figure 4: Reduced Overhead

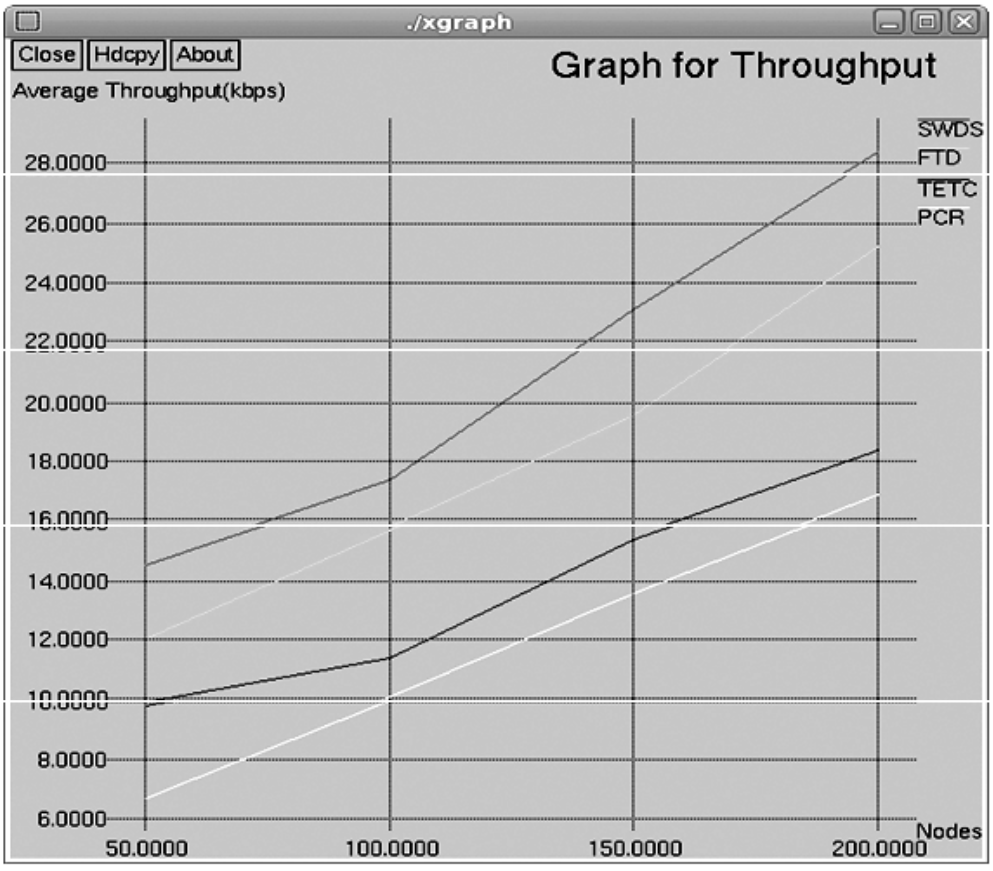

Figure 5: Network Throughput

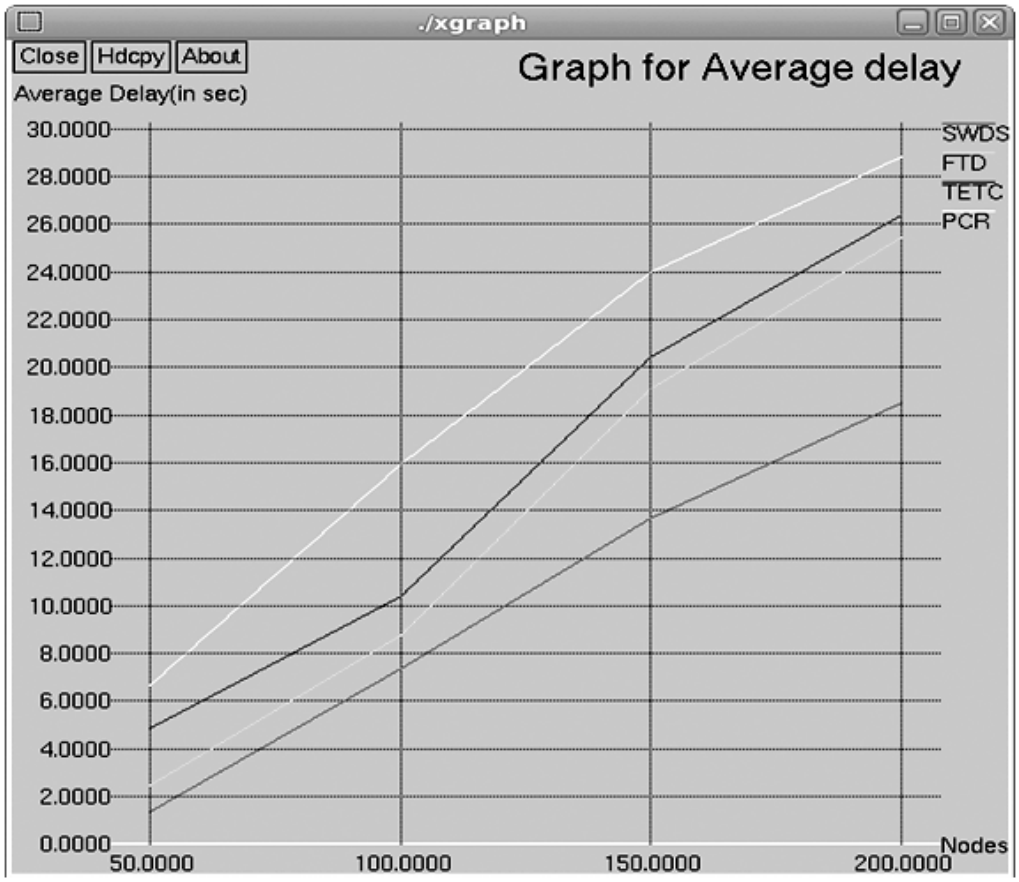

Figure 6: Average End – to – End Delay

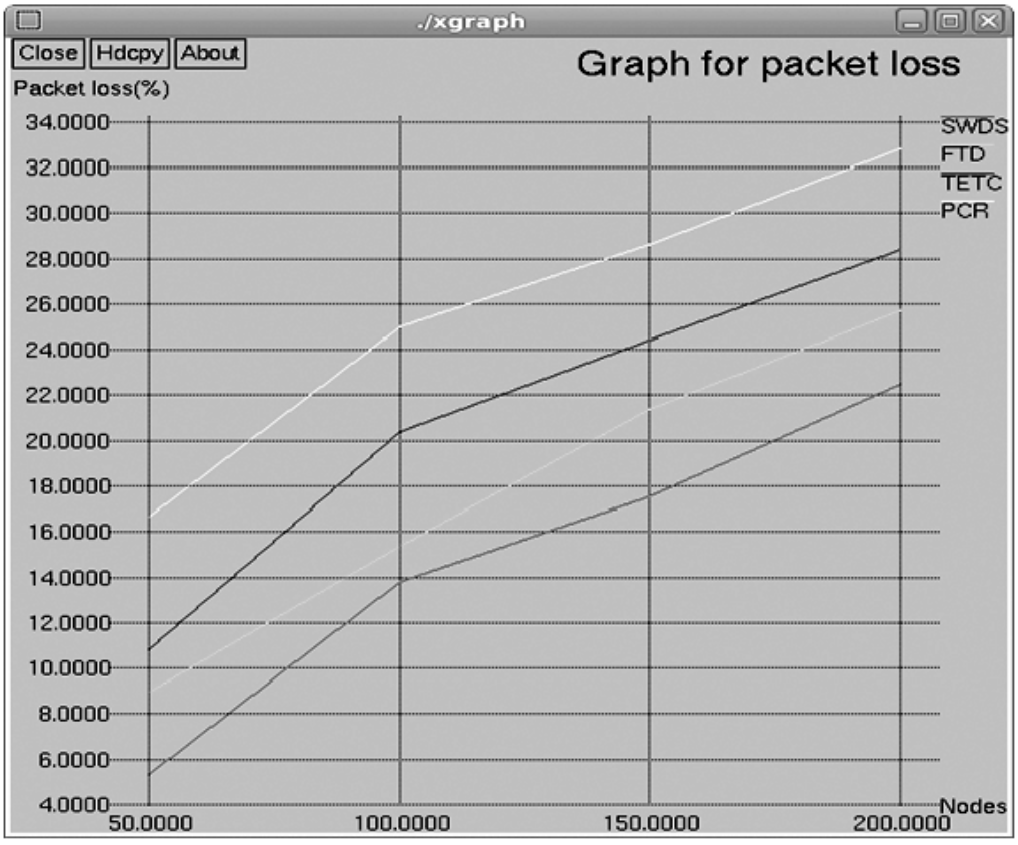

Figure 7: Reduced Packet Loss

5. CONCLUSION

Due to the presence of attacks in MANET, the nodes can be easily compromised by the wormhole attacks. The paper focuses on eliminating the wormhole attacks by designing a enhanced process of secure wormhole detection mechanism (SWDS) based on the Connection termination period (CTP) in networks. The scheme achieves better wormhole detection based on the connection termination period and the scheme is also extended for providing data integrity using UT-Updated Twofish algorithm based encryption and decryption mechanisms. The proposed SWDS scheme achieves a better misbehavior detection ratio, enhanced packet delivery ratio, minimized delay and packet losses, minimized overheads and improved throughput in terms of node count, mobility and speed. In future, the work can be extended for conserving energy during communication and also on authentication.

REFERENCES

[1] Oggier, Frédérique, and Hanane Fathi. "An authentication code against pollution attacks in network coding." IEEE/Acm Transactions On Networking 19.6 (2011): 1587-1596.

[2] Salehi, Mahmood, Hamed Samavati, and Mehdi Dehghan. "Evaluation of DSR protocol under a new Black hole attack." 20th Iranian Conference on Electrical Engineering (ICEE2012). IEEE, 2012.

[3] Yi, Ping, et al. "Performance analysis of mobile ad hoc networks under flooding attacks." Journal of Systems Engineering and Electronics 22.2 (2011): 334-339.

[4] Khalil, Issa, Saurabh Bagchi, and Ness B. Shroff. "MOBIWORP: Mitigation of the wormhole attack in mobile multihop wireless networks." Ad Hoc Networks 6.3 (2008): 344-362.

[5] DarshanSorathiya and HareshRathod, "A Review on Detection and Prevention Techniques of Wormhole Attack in MANET", International Journal of Science and Research, Vol. 4, No. 1, January 2015.

[6] Awad, Badran, and Tawfiq Barhoom. "BT-WAP: Wormhole Attack Prevention Model in MANET Based on Hop-Count." network 4.7 (2015).

[7] PrernaPriyadharshini and NeetiKashyap, "Intrusion Detection in MANETs for Wormhole Attack", International Journal of Advance Foundation and Research in Computer, Vol. 2, No. 4, April 2015.

[8] Imran, Muhammad, et al. "Analysis of Detection Features for Wormhole Attacks in MANETs." Procedia Computer Science 56 (2015): 384-390.

[9] Dubey, Neha, and Krishna Kumar Joshi. "An Approach to Detect Wormhole Attack in AODV based MANET." International Journal of Computer Applications 114.14 (2015).

[10] Nivedha and Sankara Narayanan, "Detection and Prevention of Wormhole Attack in MANET using New Fresh Algorithm", International Journal of Advanced Research in Computer Engineering and Technology, Vol. 4, No. 5, May 2015.

[11] NehaSahu, Deepak Singh Tomar and NeelamPathak, "A Modified AODV Protocol to Detect and Prevent the Wormhole: A Hybrid Approach", Vol. 15, No. 2, February 2015.

[12] Chandhandeep Kaur and Navdeep Kaur, "Impact of Wormhole Attack on the Performance of Mobility Models", International Journal of Advanced Research in Computer Science and Management Studies, Vol. 3, No. 5, May 2015.

[13] Parul Singh and Gopal Singh, "ODSRP-LET:On – Demand Secure Routing Protocol based on Link Expiration Time", International Journal of Computer Applications, Vol. 100, No. 3, August 2014.

[14] JothiTalor and Monika, "Wormhole Detection and Prevention Techniques in MANET: A Survey", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No. 2, Feburary 2013.

[15] YashpalsinhGohil, SumeghaSakhreliya and SumitraMenaria, "A Review On: Detection and Prevention of Wormhole Attack in MANET", International Jounral of Scientific and Research Publication, Vol. 3, No. 2, February 2013.

[16] Nidhi Nigam, Vishal Sharma and Mahesh Malviya, "A Novel Approach for Wormhole Detection in MANET", International Journal of Computer Applications, Vol. 63, No. 7, 2013.

[17] Zhao, Ziming, et al. "Risk-aware mitigation for MANET routing attacks." IEEE Transactions on dependable and secure computing 9.2 (2012): 250-260.

[18] G. Shanthi and Dr. A. Nachiappan, 'Adaptive QoS Multicast Routing with Mobility Prediction in MANET', IJASUC, Vol.1, No.3, 2010.

[19] Zhou, Yao, YueMing Cai, and ChengKang Pan. “A novel multicluster V-MIMO PCR scheme in large-scale Ad Hoc networks.” Science China Information Sciences 53.10 (2010): 2097-2105.

[20] Ding, Lianghui, et al. “Joint scheduling and relay selection in one-and two-way relay networks with buffering.” 2009 IEEE International Conference on Communications. IEEE, 2009.