International Journal of Pure and Applied Mathematics
Volume 114 No. 7 2017, 675-685
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

WNTFLEP-Worm Node Detection with Two Fish Algorithm based Secure Routing and Link Expiry Prediction

[1]S. Vijitha and [2]S. Bhavani

[1]Karpagam Academy of Higher Education,

Karpagam University.

[2]Dept ECE, Karpagam Academy of Higher Education,

Karpagam University.

Abstract

The security in MANET is a significant aspect due to the random deployment of nodes in network area. Distributed environment is highly vulnerable to internal and external attacks that limits network performance. Moreover frequent link disconnection produces multiple path searching thus generating more number of overheads. Our Proposed protocol concentrates on all these drawbacks . Worm node detection minimizes the interruption of data transmission and routing loss due to the presence of worms. Before sending data packets to selected neighbor its connectivity and disconnectivity is predicted using fuzzy logic and nodes with long life connections is chosen as the best neighbor to avoid packet loss . During data routing, secure data transmission is done using two fish algorithm between source and destination. So the new protocol WNTFLEP protocol provides secure communication among nodes and links with higher data confidentiality.

Index Terms: Worm node, link expiry prediction, data security with two fish algorithm.

1. Introduction

A MANET is a scattered system that does not rely on centralized servers and each node works as a router while forwarding packets to the near by nodes. This kind of vibrant network is generally useful for emergency exploration and-rescue actions. Data gets forwarded through multi hop to destination from source S_E without any infrastructural support. A frequent change in network makes irresolute and weak links among nodes. It brings packet loss and rerouting tends to add up the overheads in the network. Weak link leads to link expiry (L_E) causing unnecessary bandwidth utilization and energy loss(E_L). High delay, more energy loss, frequent link expiry and security issues can damage the network operations. In this proposed **WNTFLEP PROTOCOL (**Worm node detection with two fish algorithm based on secure routing and link expiry prediction protocol) the following is considered:

Security based data transmission between source S_E and destination D_E using TwoFish Algorithm is implemented. This algorithm provides encryption standards and has shown unbeaten encryption for manykinds of interruptions when attack is present in the network. The current key usage method is with two fish algorithm discussed with 128 bit block encryption technique shared between source and destination.

We define W_A as a malicious attack in wireless networks that is mostly tough to shield. In the W_A, an attacker captures packets at one place in the network, tunnels them to another place by creating a virtual tunnel. W_A may drop the packets or it can partially deliver the packets to the destination D_E. This kind of tunnel exists at the shortest distance between two worm nodes in the network. **WNTFLEP** eliminates $W_A$at initial route establishment itself.

This protocol concentrates on trustworthiness and link expiration time (E_T). Link failure is a major problem in MANETs. Due to frequent mobility, link expires between nodes so those node have to discover new routes to transfer the data packets

In this paper, initially network is secured from worm nodes when path is established. Route discovery packets are broadcast to the network by source S_E when it needs the path. Monitoring of the worm nodes is done by the protocol and it eliminates it at the initial level. Then using two fish algorithm data is secured and transmitted to the destination through the established multi hop path. While sending data each node runs link expiry time algorithm and chooses the best neighbor using fuzzy logic

The rest of this paper is organized as follows: Section 2 details about the proposed method used in this work. Section3explains the simulation parameters and result analysis and finally, Section4gives the conclusion summing up the features of the proposed method.

Proposed Method–WNTFLEP

Initial Network creation

Node ***Si*** istens to a HELLO message within its transmission range with edge nodes Ej enclosed with its identification (ID) and broadcasting time(BT_S), thus node s_i constructs an edge nodes list (E_L). Node s_i also sends a HELLO message enclosed with its ID and BT_S When the receiver gets HELLO packets it updates E_L with new neighbors entry. At the commencement each node has E_L with which it forms a connected network in the given area .

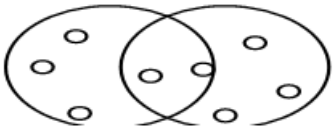

Figure 1: Transmission Range E_L Nodes Neighbor set construction

Attack of WORM Node Model

To set up an attacker model W_A, an attacker places a minimum of two nodes at different places in the network. The two malicious nodes create a tunnel and attempt an attack by passing the data packets through the tunnel. The attacker can transport the packets faster than the usual network. Moreover the data packets are also tunneled through T_{NL}. This T_{NL} allows signals to move from W_N to tunneled nodes faster than the normal link. W_A or the attacker section is built with high transmission range and bandwidth either with wired or wireless link. Control packets or data packets are exchanged from W_A through the T_{NL}. When S_E has to communicate with its D_E, S_E increases its broadcast ID and begins path invention by propagating a route request (RREQ). RREQ packet moves from each node in the path up to the destination D_E. Each intermediate node I_N rebroadcasts that RREQ to its E_L nodes. W_A attack can simply be initiated by the attacker exclusive of network knowledge or negotiating any genuine nodes or security systems. After detection each node updates the attack flag in its E_L .Its tedious to control the participation of these types of attacker nodes W_A. So we have to ensure secure routing of control and data packets. W_A can exist in the network even if all transmissions are secured. It can act as secretor bare type attack. In secret W_A hide their presences in network, legitimate nodes are unable to know their survival in network. In bare type W_A legitimate nodes knows the involvement of misbehaving nodes during forwarding, but is unsure to eliminate it. This kind of W_A node creates a false impression that S_E and D_E are placed in one hop distance. S_E sends the packet,

which is received by W_A1 and without modifying the packet T_{NL} it to the W_A2. W_A2 forward that data packet to the D_E without any change. D_E constructs N_{Info} table and checks the enclosed data structure. W_A1 and W_A2 does not enclose the L_C, E_R and D_{ist} with previous hop. In bare type W_A model it does not change the structure of the packet, but it includes its own routing information into the header of the packet. $\boldsymbol{S_E}$ sends the control packet to establish path captured by the W_A1. $W_A1$knows the previous node hop count as 1, it include its hop count as 2 and forwards to W_A2. W_A2 identify previous hop count as 2, so that W_A2 update its hop count as 3 and sends that to D_E. So that the route established as $\boldsymbol{S_E}$, W_A1, W_A2, D_E.Some legitimate nodes may not be located in the nearby location of W_A. Some normal nodes are located in the scrutiny of W_A1.Few nodes can be placed in the sight of both the attackers W_A 1 and W_A2. Basically W_A does not obey the rules of the protocol. It aims to reach the D_E as the initial routing path node ;this behavior eliminates original nodes' RREQ to reach destination D_E at first. Normally the second routing packet that arrives at D_E may get dropped. This behavior spoils and fades the security in networks. In W_A detection model time variation based data transfer is verified.

Route Establishment in Network

Network region is chosen as a bound for graph $G=\{N,E\}$,where $N=\{n_1,n_2,.....n_n\}$N defines the nodes in the network and group of neighbors defined as E, $E=\{e_1,e_2.....e_3,e_4,.....e_n\}$. At initial, $\boldsymbol{S_E}$ verifies its routing table (T_R) to find valid next hop neighbor to reach D_E . Each node maintains E_L to keep a record of its neighbors, T_R to store its valid data transmission path neighbor entry and block list (B_L) to store worm node W_A behavior to eliminate attackers from E_L and T_R.

If $\boldsymbol{S_E}$ wants to send a packet to D_E then the protocol looks for the route and creates the connection in order to send and receive the data packet. The path discovery generally occurs by flooding the RREQ packets all over the network .RREQ packet enclosed with time stamp (R_{ST}) current location (L_C), remaining energy (E_R) and its packet sequence number (S_{No}) through the wireless medium. Each intermediate node (I_N) receives and rebroadcasts RREQ until it reaches the final D_E. While rebroadcast of RREQ is done by the I_N, it encloses the distance (D_{ist}) with previous node as mentioned below, distance calculated between each neighbors in propagation model. Let i and neighbor j have coordinates of $(x1, y1)$ and $(x2, y2)$ in that order as nodes

positioned at network region. D_{ist} between node i and j is computed as

$$(d_{ist}) = \sqrt{|x1 - x2|^2 |y1 - y2|^2}$$

L_C taken as current coordinates of $(x1, y1)$ and $(x2, y2)$ and the E_R of node is computed as

$$E_R = E_i - (Tx_{EN} + RX_{EN})$$

where E_i denotes the opening energy of the node , Tx_{EN} the transmission energy, RX_{EN} the reception energy respectively till $D_E$via multiple nodes. D_E gathers all path nodes' information and stores them in a table N_{Info}. N_{Info} holds the path node ID, each nodes' D_{ist} with previous hop, each nodes E_R, L_C, and S_{No}. Then D_E sends route reply message (RREP) enclosed with N_{Info} back to S_E. After path establishment S_E will be able to send its data to the D_E. Before sending data packet S_E validates the N_{Info} about all node information placed in path. If N_{Info} is empty or filled with unstructured packet header that complete path nodes are rejected by S_E considered as W_A path and those path nodes ID are announced as suspicious attackers present in the path. Each node maintains a node block list B_L. All suspicious node entries are stored in B_L. In future, all genuine nodes check B_L before making communication to eliminate suspicious node entries from T_R.

Detection of Worm Nodes

During route discovery RREQ packet sent by S_E is enclosed with R_{ST}, L_C E_R, and S_{No}. I_N also forwards the RREQ message and includes its R_{ST} L_C E_R, S_{No} D_{ist} along with the previous node information. When RREQ moves, it sets up the reverse path entries back to S_E. If a I_N has next hop for the preferred D_E in its T_R, it matches up the destination S_{No} in its T_R with that in the RREQ. If the D_E S_{No} in its T_R is lower than that in the RREQ, it re-broadcasts the RREQ to its E_L nodes. When the RREQ arrives at D_E, it creates N_{Info} and encloses it into the RREP. As per reverse path RREP travels back to the S_E,.When the I_N receives the RREP,it gets forwarded until the S_E is reached. In each reverse path node stores the RREP time as R_{PT}. It estimates the time difference of these two control packets called R_{Diff}. To calculate R_{Diff}, all the nodes need to update two control packets R_{ST} and R_{PT} the forwarding time and receiving time of the RREQ and RREP. The R_{Diff} produces travelling time of routing packets from S_E to S_E.If routing packet are passed through W_A1 and W_A2, path established is

,S_E, W_A1, W_A2 and the R_{Diff} values are computed as above, then the R_{Diff} provides time difference between original path and worm path. If worm node link is present in the path R_{Diff} < normal path. Computation of energy E_{Diff} will produce the summation of normal path energy utilization (NP_{EU}) and summation of worm node path energy utilization (WP_{EU}) variations.

$NP_{EU} = \Sigma NP_{EUi}\ i \in \forall$nodes in path

$WP_{EU} = \Sigma WP_{EUi}\ i \in \forall$nodes in path

$E_{Diff} = \max(NP_{EU}, WP_{EU})$

If E_{Diff} value = 0 it considers that path as worm path because worm node does not enclose energy utilization of path.

Worm Nodes Detection Model:When the S_E gets RREP, it begins worm node detection. Compares R_{Diff} between all nodes in path .In all normal node path the R_{Diff} will be in the same range with small changes. Presume, if the path is constructed with W_A, it can find high variations in the path difference with a suspicion that there is a wormnode in path.

Elimination based : Initially when network starts, each node maintains the E_L and T_R. If the R_{Diff} is significantly lower than the standard R_{Diff}, then assume worm node link is established. To assure that, network setup can be re altered. W_A tries to capture more E nodes in its coverage. So there is a need to validate each node neighbor connectivity C_N count ,area (A) of the network region, e number of nodes in that region ,r node coverage radius.

$$C_{N\ ?} = \left(\left(\frac{(e-1)\pi r^2}{A}\right)\right)$$

Based on E_{Diff}, R_{Diff}, N_{Info}, $C_{N\ ?}$, S_E concludes worm node path and broadcast the W_A presence in to the network nodes. Using this all normal nodes update W_A entries in B_L to eliminate those nodes in further routing path.

Link Expiration Time Computationduring Data Transmission

During data transmission by physical layer it detains the packets and computes data route solidness state (DRSS) based on the transmission range and signal strength at receiver end. S_E broadcast RREQ, when it arrives at network layer, D_{ist} computation is executed between S_E and E nodes. Apart from D_{ist},node movement is taken as mobility inside the network and relevant power variation depends on the distance changes continuously monitored by nodes to know the deviation of the neighbors. Based on the angle and deviation changes node can estimate the neighbor disconnection period as link expiration time (L_E). Power variation while communicating between two nodes is called as signal strength

(SSR) computed at receiving node, this is computed at the receiver end based on Tx_{EN} and RX_{EN} . SSR provides power variation based distance estimation as.

$$SSR = \frac{\sqrt{(\mathrm{Tx}_{EN}\, X\, \lambda^2)}}{(4 \mathrm{x} \pi)^2 \mathrm{x} \mathrm{L} \mathrm{x} \mathrm{RX}_{EN}}$$

L is taken as the channel path loss and λ^2 considered as the communication wavelength. Along with these two parameters link expiry time ($\mathrm{L_E}$) is estimated from the neighbor distance variation time, as a third parameter. Also speed(S_D) of node is computed based on its location changes due to mobility.SSRvariation between e_1, e_2 is estimated while the nodes are communicating.So $\mathrm{L_E}$ can be found from E_L to get the neighbor availability.

$\mathrm{L_E} = \mathrm{R}_{ST} - \mathrm{E}_L$ expire where E_L gives the changes of neighbor list with exact time. A simple fuzzy estimation gives the accuracy of neighbor E_T. As per fuzzy input SSR changes, $\mathrm{L_E}$, S_D are given by fuzzification algorithm. When data packet is routed through the neighbors as per T_R ,before transferring data update,$\mathrm{L_E}$ based fuzzy output selects long life neighbor as next node to route the packets. In order to choose high priority neighbor to avoid link disconnection while the valuable data transfer is performed, $\mathrm{L_E}$ prediction avoids unnecessary link expiry that eliminates frequent rerouting. This minimized the overheads in network. Overhead reduction increases the network performance.

Secure Data Transmission Using Two Fish Algorithm

Anonymous malicious behavior can attack network transmission any time. Key dependent S-boxes rules, is constructed with 128 bit keys to confirm that all the S-boxes arecertainly strong. This gives ability to make strong steady, S-boxes along with furtive S-boxes. Moreover Twofish algorithm has no poor key support.

Always the subkeys are carefully calculated, using S-box building rules, to avoid various key attacks and to give good key integration. During this key building time it is designed in tandem with the cipher. The 1-bit turning round is calculated to split up the byte arrangement; else, the whole thing operates on bytes. This process exists to disturb cryptanalysts. Because eight-XOR are less than a round, it makes sense to leave them. Several presentation tradeoffs exists between key building time and encryption time. Twofish generate the key and create the key dependent S-boxes and time based sub keys as it is of high speed.

Using Twofish algorithm encrypts huge volume of plaintext small blocks with fast altering keys. These methods make the Twofish algorithm to ensure a different way to encrypt data in one way and decrypt it in another way. For

making 128bit key additional modification is not necessary to get the keys.

Simulation Parameter and Result Analysis

For simulation purpose a network area of 800sqmx800sqm was considered with 100 nodes with initial energy 100Joules with a transmission power of 0.06Mw and reception power of 0.03Mw.The 802.11 MAC was chosenwith 512 bytes of poacket size.

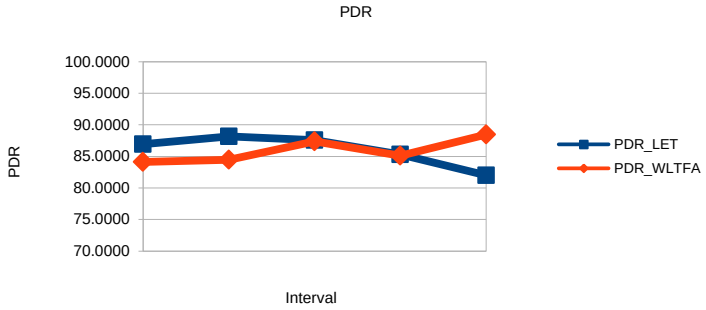

Figure 2: Interval Vs PDR

Fig. 2shows the packet delivery ratio(PDR) with intervals for LET and WNT**F**LEP with changing time. Proposed worm detection protocol shows high packet delivery ratio (PDR) after detection and elimination of the attacker from path. Also link expiry computation gives strong path without attacker. This estimation produces less packet drop so the PDR is increased.

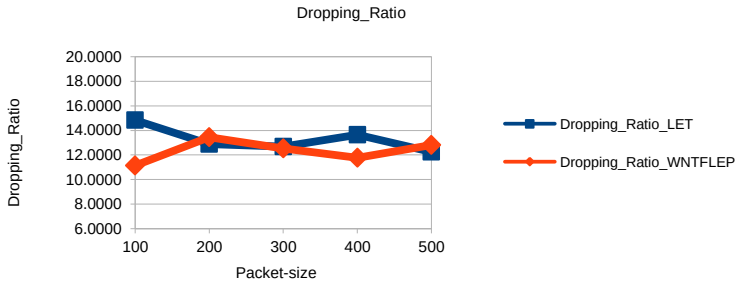

Figure 3: Packet size with dropping ratio

In fig 3 network isanalyzedfor packet dropping ratio by changing packet size variation.Packet dropis reduced in WNT**F**LEP than LET. This is due to the prediction of $L_E$using fuzzy logic.

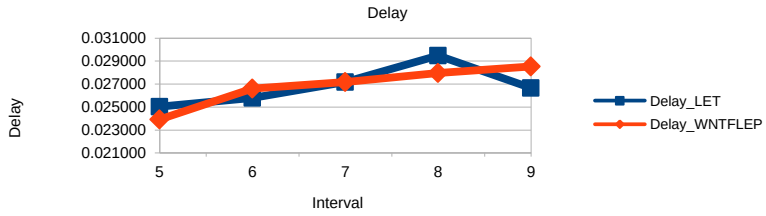

Figure 4: Interval vs delay

Fig 4 explains the output for delay. The WNT**F**LEP end-to-end delay is less than LET. This is due to the fact that the network is secure with Twofish algorithm with link expiry computation based on route selection. In fig 3 network analyzed packet dropping ratio by changing packet size variation. Packet drop reduced in WNTFLEP than LET. Small variations can be seen in the graph because of link expiry and fuzzy logic detection.

2. Conclusion

In this proposed WNTFLEPPROTOCOL ,the control packets are reduced and the packet delivery counts received at destination are increased .L_E estimation between nodes in path using fuzzy logic minimizes the re routing. Worm node detection and elimination in path during route establishment minimizes packet loss and secures network establishment. In addition data is secured by Twofish algorithm. In future inference reduction at channel can control the deviations in the current protocol

References

[1] John Preskill, wormholes in space time and the constants of nature, U.S. Department of Energy under Contract No. DE-AC0381- ER40050.24 (1988).

[2] Vani A., Sreenivasa Rao D., A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In Ad Hoc Wireless Networks, International Journal on Computer Science and Engineering (IJCSE) 3(6) (2011).

[3] Dezun Dong, Mo Li, Yunhao Liu, Xiang-Yang Li, Xiangke Liao, Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks, IEEE/ACM Transactions on Networking 19(6) (2011).

[4] Md. Ashraf Uddin, Mamun-or-Rashid, Link Expiration Time-Aware Routing Protocol for UWSNs, Hindawi Publishing Corporation Journal of Sensors 9 (2013).

[5] ZHI ZHANG, Networked RFID Systems for the Internet of Things, KTH School of Information and Communication Technology SE-164 40 Kista, Stockholm SWEDEN (2013).

[6] PurnimaGehlot S.R, Biradar B.P. Singh, Implementation of Modified Twofish Algorithm using 128 and 192-bit keys on VHDL, International Journal of Computer Applications 70(13) (2013).

[7] Vikaskumarupadhyay, RajeshKShukla, WPAODV: Wormhole Detection and Prevention Technique, Int. J. Advanced Networking and Applications 05(03) (2013), 1922-1927.

[8] Parul Singh, GopalSingh, Security Issues and Link Expiration in Secure Routing Protocols in Manet: a Review, International Journal of Advanced Research in Computer and Communication Engineering 3(7) (2014).

[9] Much Aziz Muslim, Budi Prasetiyo, Alamsyah, Implementation Twofish Algorithm for Data Security in a Communication Network Using Library Chilkat Encryption Activex, Journal of Theoretical and Applied Information Technology 84(3) (2016).

[10] Gopal Singh, Deepak Saini, Rahul Rishi, Harish Rohil, Role of Link expiration time to make reliable link between the nodes in MANETs: A Review, International Journal of Applied Engineering Research 11(7) (2016).

[11] Aparna K., Jyothy Solomon, Harini M., Indhumathi V., A Study of Twofish Algorithm, International Journal of Engineering Development and Research 4(2) (2016).

[12] Gubbi J., Buyya R., Marusic S., Palaniswami M., Internet of Things (IoT): A vision, architectural elements, and future directions, Future generation computer systems29(7) (2013), 1645-1660.

[13] Al-Majeed S.S., Al-Mejibli I.S., Karam J. Home telehealth by internet of things (IoT), IEEE 28th Canadian conference on Electrical and computer engineering (CCECE) (2015), 609-613.

[14] SomayyaMadakam, R. Ramaswamy, Siddharth Tripathi, Internet of Things (IoT): A Literature Review, Journal of Computer and Communications (2015).

[15] SamiaAllaoua Chelloug, Energy-Efficient Content-Based Routing in Internet of Things, Journal of Computer and Communications (2015).

[16] Lazos L., Poovendran R., Meadows C., Syverson P., Chang L.W., Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach, Wireless Communications and Networking Conference 2 (2005), 1193-1199.

[17] Maheshwari R., Gao J., Das S.R. Detecting wormhole attacks in wireless networks using connectivity information, 26th IEEE International Conference on Computer Communications (2007). 107-115.

[18] Xu Y., Chen G., Ford J., Makedon F., Detecting wormhole attacks in wireless sensor networks, Critical infrastructure protection (2007), 267-279.