RESEARCH ARTICLE OPEN ACCESS

An Efficient Approach to Detect & Prevent the Tunneling Attack through Hybrid Algorithm in Wireless Sensor Network under IAODV Protocol

Somya Gupta, Chanchal Sharma
Research scholar, Department of Computer Science, Suresh Gyan Vihar University, Jaipur
Assistant professor, Department of Computer science, Suresh Gyan Vihar University, Jaipur
Corresponding Author: Somya Gupta

ABSTRACT: In the era of wireless communication system as the application development scenario is increasing rapidly. Vanet is basically a vehicular ad hoc network which is defined in the IEEE 802.11p Standard for better adaptability in the wireless network environment that basically provide the communication among both vehicle to vehicle and vehicle to infrastructures because having the distributed environment, security emerges as an important issue. The transmission of the data is performed under the untrusted network environment. The authenticity is vulnerable to different security attacks. Wormhole attack is one of the serious kind of attack on the wireless sensor network In which packets are captured by a malicious node that perform tunneling from one location to the another location and also transmit them into the established network. In this paper we discuss about the efficient method to detect wormhole tunneling by adding the Data packet leashes with some advancement by including the packet status along with it which is authenticated by the two secure cryptographic algorithms RSA combine with the Digital Signature Algorithm. The packet broadcasting is performed by the efficient IAODV routing protocol.

Keywords: Packet leashes, Digital signature, RSA, IAODV.

Date Of Submission: 30-09-2019 Date Of Acceptance: 14-10-2019

I. INTRODUCTION:

Vanet has a distributed infrastructure so it has to manage all the security and privacy issues in the network during the communication between distributed nodes in the vehicular ad-hoc networking In vanet there are various attacks like wormhole attack, Sybil attack, and man in the middle attack, jelly fish attack, denial of services (DOS) attacks and attacks that affect the authentication of the network. So considering all these issues in the vanet network there are some method for preventing and detecting all these malicious attacks in the network to make the vehicular ad hoc system more secure and efficient. The main reason for the security of the network is to hide the information about the original identity of the drivers so that malicious nodes could not misuse.

1.1 PARAMETERS OF SECURITY IN VANET:

For the security of vanet network some parameters of the security are defined which include its specific properties and criteria to provide security attributes. Here are those security attributes for any network. [1]. Here are some security parameters in the following description:

A. Authentication: This attribute ensures that the message or the information is sent by an authenticated user.

B. Integrity: It gives the assurance to the user that he received the original message or data. The data is not altered by any malicious attacker.

C. Confidentiality: Through the confidentiality the privacy of the data maintains. Some kind of sensitive information should exchange in an encrypted manner.

D. Non-repudiation: It is like an assurance which cannot be denied by the user which prevents the attacker to deny.

E. Availability: It allows all the resources available to the valid users when they requires.

1.2. TUNNELING THROUGH WORMHOLE ATTACK

In the wormhole attack the communicating network is surrounded by more than one malicious vehicles or nodes in the system. These malicious nodes build a tunnel within a network and sends malicious messages from one node to another node through the tunnel. The malicious nodes keep the control of the whole network system.

So continuously exchanging of these malicious messages makes the communication system inconsistent. The process of the establishment of the tunnel in two ways .The first method is that tunneling creating within the Out of band channel and the second way is in band channel. These ways creates an illusion because the tunneled data packet is arrive very Quickly or it takes very less hop count in compare to the usually process of transmission .So it become hard to detect the malicious routs. Various kinds of attacks can be formed like replay attacks, Eavesdropping attacks etc. Here in the following figure the tunneling is established by two attacker nodes during the packet transmission.

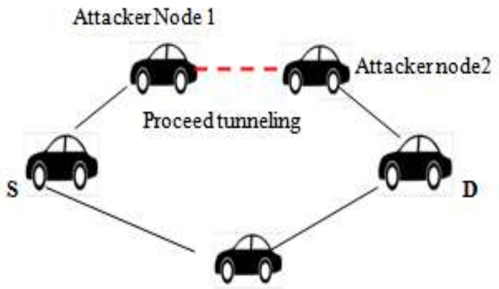


Fig1: Proceed tunneling by malicious node 1 and node 2

We can classify the types of wormhole attacks according to the visibility of the attacker nodes on the transmission routs or the behavior of the attacker nodes to forward the data packets .so it can define by the different categories like open wormholes, half-open wormhole and the third is closed wormhole attack. In the open wormhole attack the attacker node is known by the other nodes in the network and they would pretend that the attacker nodes as their direct neighbor node. But in the case of half-open wormholes the attacker can only perform the tunneling the data packets within the network from one side to another side and rebroadcasts them without doing any modification or changes to the packets. In the closed wormhole attacks, the source and the destination nodes are shown as both are far away as only one hop from each other, and all the intermediate nodes in the networks routs are kept as hidden nodes. [1]

II. RELATED WORK:

Wormhole attacks can be easily launched on the network security system because of the non centralized infrastructure and it is difficult to detect within the distributed network. More ever various wireless sensor network routing protocols deploy the different cryptographic techniques or other solutions like directional antennas, packet leashes techniques, clock synchronization, DELPHI technique [2] etc. to prevent the network from the unauthorized access with this tunneling attack. Here are some methods including related work presented by different authors to detecting or preventing the wormhole attack from the wireless sensor network.

Hon Sun Chiu et al [2] In this paper the author presents a new method that is DelPHI, which is called as delay per hop indication. In which the author detect the wormhole attack by observing the delay between the sender and the receiver during the transmission of the packet. Accordingly this method of detection does not require any type of hardware resources and the synchronized clock.

Saurabh Gupta et.al [3] in this paper the author used a WHOP algorithm which used packet hound for detecting the wormhole attack in the wireless network. With this algorithm it detect the tunnel by counting the number of hops between the nodes & evaluate that the hop difference between the intermediate node are acceptable or not.

Seyed Mohammad Safi et.al [4] Authors proposed a novel approach for the avoidance of the wormhole attack in the vanet network. This avoidance technique includes the packet leashes and the heap method for the wormhole attack occurs during the routing of the protocol.

In the proposed method the wormhole attack can be prevented by detecting the malicious node in the communication network because the attack is happens through two or more than these malicious nodes. This attack basically interrupts the routing network especially the networks that uses on demanding routing protocols like AODV and DSR.
Hichem Sedjelmaci et.al [4] Authors proposed frame work which is an intrusion detection system for vehicular network (IDFV) which secure the wireless network against the various routing attacks like

Wormhole attack, packet duplication occurrence while transmission and black hole attack etc. this IDFV framework applies a secure reputation method for the assessment of the trust level of the vehicles along with the sensor networks. This frame work basically evaluates the system with the high detection rate and low false rate accordingly.

III. PROPOSED WORK

In the tunneling attack, the data packet or information is received by a malicious node called as attacker at a particular location point and it tunnels those data packets to the different place and replays those packets into the whole wireless transmission network. These attackers can transmit the information bit by bit from the data packet instead of waiting for the whole packet to be forwarded so that it could maintain the minimization in the delay .So this would be more harmful and not so easy to detectable in the wireless sensor network.

The proposed methodology is basically based on the ad hoc on demand routing protocol AODV protocol is worked as a reactive routing protocol in which the nodes present in the network worked as the routers. When it is necessary to send the data within the network they obtain the rout by maintaining the routing table. The approach of IAODV protocol [5] is worked on the statement that is as “limited source routing up to two hops with the backup routs."[5]

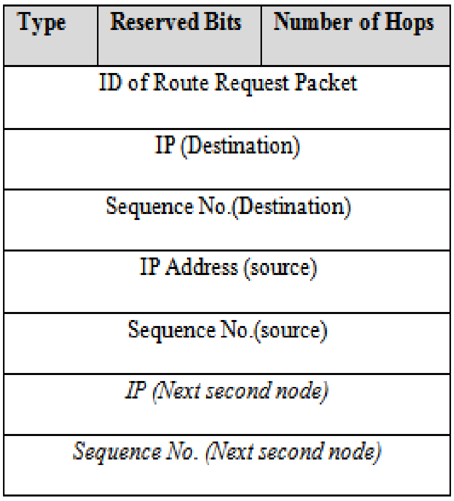
Basically this extended protocol merges the features of DSR and AOMDV protocol. In the basic Ad hoc on demand routing protocol, it gives a surety by giving the information timely with a highly accuracy.

3.1 Improved Rout Request (IRREQ) And Improved Route Response (IRREP) Packets

The secure routing phase is complete with two phases in which first is rout discovery and rout maintenance is the second and last phase. During the discovery of the transmission rout the improved route request IRREQ phase is extended in a way to create the backup routes from the source to the destination that if occurrence of any primary route failure, the source node can use the backup routes for data transmission. In the proposed routing protocol it includes the additional address of the next node of the communication network.

Here the design of the updated & improved route request packet (IRREQ) structure which contain the IP address of rout request packet, IP address of destination address, sequence no. of rout request packet and addition of IP address of next node with is sequence no.

The Structure of the packet with these parameter is as shows in the following table:



Type	Reserved Bits	Number of Hops
ID of Route Request Packet		
IP (Destination)		
Sequence No.(Destination)		
IP Address (source)		
Sequence No.(source)		
IP (Next second node)		
Sequence No. (Next second node)		

Fig2: Rout-Requesting table of improved transmission protocol.

3.2. Prevention From The Tunneling Effect

After the routing sequences it become a big issue to protect the data packet securely from the different networking attacks like Wormhole, DDOS attacks, jellyfish attack etc, which we are already discussed before because of having distributed infrastructure. So to prevent the transmission network over the Wormhole tunneling the packet leashes are very effective mechanism to deal with wormhole attack over the wireless network.

This leashes technique is categorized by two different methods. In this geographical leashes all nodes which have loosely synchronized clock along with them & these node must be aware of their location so accordingly if a data packet is sending by a nodes, P_{src} must include its location an the time T_{sen} which compute the ±Δ and V ,the upper bound on the velocity of node through the following equation: $DSR \leq | \, | P_{src} - P_{rec} | \, | + 2V.(T_{rec} - T_{sen} + \Delta) + \delta$

Where DSR = distance between the sender and the node itself in the communication network.[7]

On the other hand the temporal leashes used the tightly synchronized clock which include the concept of computing the maximum difference (Δ) between any two nodes within the transmission network and which is necessary to known by all of the nodes participated in the communication network. We uses these method to control over the wormholes created by the malicious nodes through under the condition in which the packet cannot be able to traverse further than the particular given distance denoted by L within the communication network. Every node in the network must be synchronized up to the **Δ.** So $L > L_{min} = \Delta.c$,

Where Δ=maximum time synchronization error & C = the wireless signal speed over the communication.

When a packet is send by a sender node at a time Tsen then a time of its expiration must be assigned as $T_e = T_{sen} + L/C - \Delta$, when the receiver receives the data packet if the temporal leashes is expired (means Trec > Te). [7] It drops this packet in that case.

3.3. A Hybrid Authentication Approach For Securing Data Packets

The use of temporal leashes is not enough for securing the communication network from the malicious nodes to create tunneling. The expiration time must be authenticated so it becomes secure from intrusions set up by the attackers. Basically we uses the concept of the hybrid cryptographic technique which merge the more optimal features of two secure cryptographic algorithms which is the RSA emerging with the concept of digital signature algorithm.[8]

RSA works on the public key cryptography including two basic functions which are encryption and the process of decryption and the digital signature algorithm generate the digital signature and validate it. The hybrid feature wants to maintain the efficiency of bits so it includes the 1024 bits for RSA with the 512 bits DSA algorithm that leads the transmission of the message more secure as compare to previous proposals related to the security.

In this hybrid algorithm the key generating procedure is manage under the trusted authority. A pair of public and the private key is provided to every user which participates in the communication network. The next process is performing the cryptographic algorithm with the help of these key pairs.

- RSA Algorithm: Perform encryption and decryption
- Digital Signature: Verification process

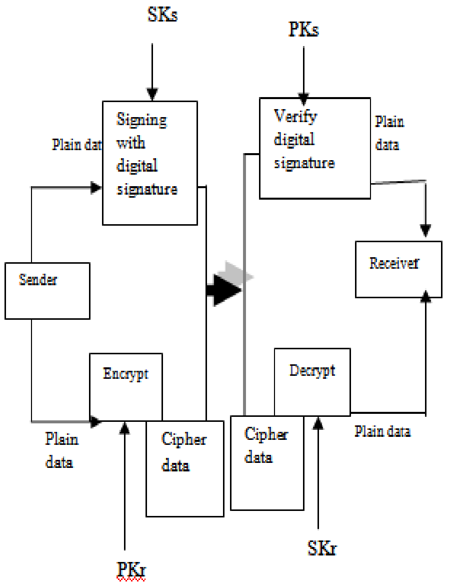


Fig3: Functioning of the used secured hybrid algorithm.

These pairs of keys are used to encrypt and signing the data packet and after verifying it for the decryption of the data packet. When every nodes have their pair of keys & any node will send data where the encryption process is done through the public key of the receiver node and it digitally signed by the private key of the sender node and on the other hand receiver node receive the encrypted data packet which can be only decrypted by the public key of sender node. The verification procedure with the digital signature is done by the public key of sender node. Data is received when the digital signature is found valid as the whole procedure is shown in the described figure. So we go through this procedure to be more secure against the wormhole attack.

3.4. Process Flow Of Transmission Under Wireless Sensor Network

The process is starts form the secure routing protocol which additionally manages the temporal leash with its deadline time to detect the tunneling created by the malicious node and eventually performed the wormhole attack in the transmission network which obviously affects the security parameters during communication within wireless sensor networks. Here is the flow of procedure under IAODV routing protocol with the addition of packet leashes which is used to detect and prevent the network from the various attackers.

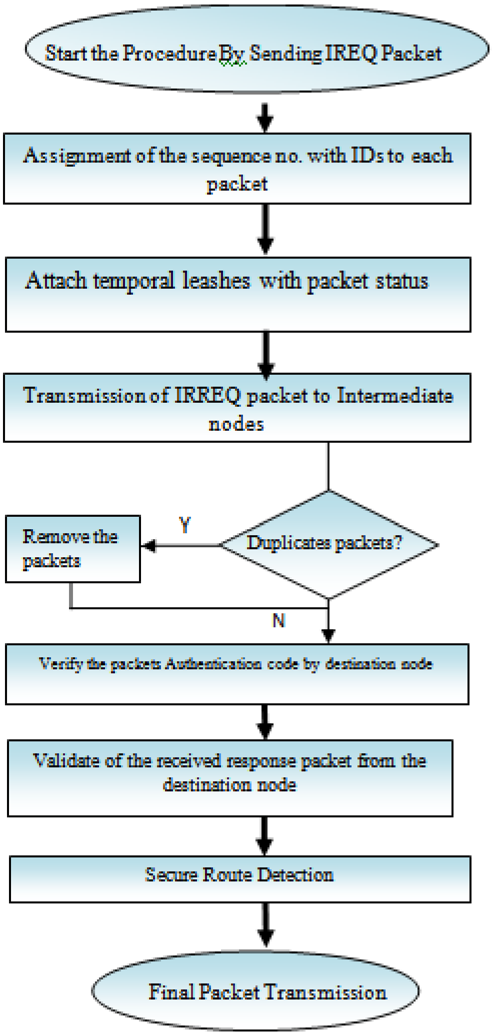

Start the Procedure By Sending IREQ Packet
Assignment of the sequence no. with IDs to each packet
Attach temporal leashes with packet status
Transmission of IRREQ packet to Intermediate nodes
Duplicates packets?
Y
Remove the packets
N
Verify the packets Authentication code by destination node
Validate of the received response packet from the destination node
Secure Route Detection
Final Packet Transmission

Fig 4: Secure Rout flow to control over malicious nodes in wireless sensor network.

IV. SIMULATION & RESULT:

The implementation of wormhole attack prevention is done under the network simulator2 (NS2).Basically it has a UNIX based open source environment, generally using TCL language for scripting. Through this approach of improved routing protocol the packet deliver rate is maintained with the addition of hybrid cryptographic algorithm as compare to basic ad hoc routing protocol under high traffic scenario. We compare the result by calculating some factor like end to end delay and throughput. Here in the following figure the analysis graph of throughput, this basically refers to the average data rate of successful message delivery over a specific communications link. From the results, proposed prevention method gives more throughput than the existing one as shown following measured in bits per second (bps).

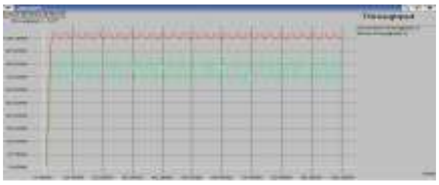


Fig5: Throughput gained by the proposed prevention method.

Packet Delivery Ratio (PDR) is a number of successfully received packets to the total number of packets sent by sender which includes re-transmissions of the packet also. In the second simulating graph, red line indicates the energy consumption in the prevention method, where as green is for attacker method. According to this result, proposed method PDR is higher than before.

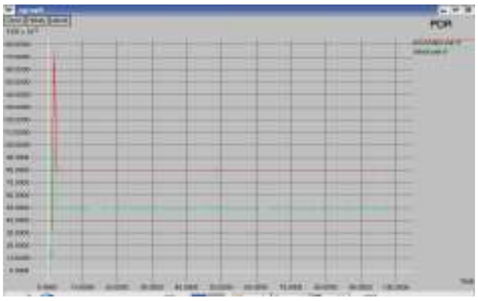


Fig6: Calculated PDR by the proposed prevention method.

End to End Delay is the final parameter to analysis of the time taken for a packet to be transmitted across a network from source node to destination node that depends on number of hops and traffic congestion on the network. In the results end to end delay is has lower value in proposed method as compare to the previous one

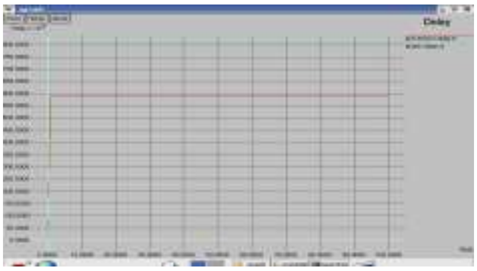


Fig7: Analyzed minimum end to end delay

As the following graph shows that end to end delay during packet transmission is improved by using IAODV protocol instead of basic AODV protocol while applying hybrid algorithm for handling security issues from wormhole attackers.

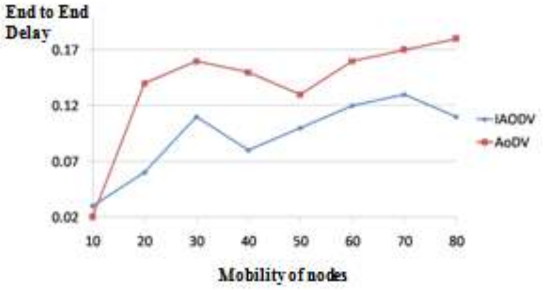


Fig8: Performance analysis in term of end to end delay between IAODV and basic AODV protocol

V. CONCLUSION & FUTURE SCOPE:

In wireless sensor network, security becomes very important issue because of having its distributed kind of environment so in this paper we worked on the security related issues like tunneling attack and proposed some improved routing protocol with packet leashes technique & secure it by a hybrid cryptographic approach. Through this implementation flow the packet delivery rate is much improved with efficient way. We can further implement some more advance features which can take less time to detect wormhole attacker to find secure routs and reduce delay between packet transmissions even more efficiently.

REFERENCES

[1]. Tareq Emad Ali, Layth A. Khalil,l dulaimi Yamaan E. Majeed , Review and Performance Comparison of VANET Protocols: AODV, DSR, OLSR, DYMO, DSDV & ZRP, 2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AICMITCSA) IRAQ (9-10) May

[2]. H.S. Chiu and K.S. Lui. DELPHI: wormhole detection mechanism for ad hoc wireless networks. 1st International Symposium on Wireless Pervasive Computing, pages 6–11, January 2006.

[3]. Saurabh Gupta, Subrat Kar, WHOP: Wormhole Attack Detection Protocol using Hound Packet, 2011 International Conference on Innovations in Information Technology.

[4]. Seyed Ali Sharifi and Seyed Morteza Babamir, A New Approach to Detecting and Preventing theWorm Hole Attacks for Secure Routing in MobileAd-hoc Networks based on the SPR Protocol IEEE.

[5]. Dharmendra Sutariya, Dr. Shrikant Pradhan, An Improved AODV Routing Protocol for V ANETs in City Scenarios IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012

[6]. Shahjahan Ali, Prof. Parma Nand Prof. and Shailesh Tiwari , Secure Message Broadcasting in VANET over Wormhole Attack by using Cryptographic Technique, International Conference on Computing, Communication and Automation (ICCCA2017)

[7]. Y.C. Hu A. Perrig and D. B. Johnson. PACKET LEASHES: A defense against wormhole attacks in wireless ad hoc networks. IEEE INFOCOM, pages 1976–1986, 2003.

[8]. Farah Jihan Aufa, Endroyono and Achmad Affandi Security System Analysis in Combination Method RSA Encryption and Digital Signature Algorithm, In 4th International Conference on Science and Technology (ICST 2018), Yogyakarta, Indonesia.

Somya Gupta" An Efficient Approach to Detect & Prevent the Tunneling Attack through Hybrid Algorithm in Wireless Sensor Network under IAODV Protocol " International Journal of Engineering Research and Applications (IJERA), vol. 9, no. 10, 2019, pp 61-66