Believer Based Protected and Efficient Routing in Pervasive Network

J. Lenin[1]
Research Scholar M.S University Tirunelveli

M. Punithavalli[2]
Director –MCA, Sri Ramakrishna Engineering College, Coimbatore

Abstract
A Pervasive Network is one in which the estimation of the capability of the nodes to arrange themselves autonomously in the network environment and exchange information through these networks. All types of ad-Hoc networks come under pervasive network. In this dynamically changing environment, we cannot provide security in the best manner. So, we propose Believer based protected and efficient routing (BBPER). In our proposed system, each autonomous node present in the pervasive network maintains the list of believer nodes in its transmission range. Initially, each node is preloaded with the randomly generated prime number. The believer node is selected by sending a confront message as a puzzle to its neighbor. The node which has the same prime number alone would reply correctly. Based on this criterion every node selects its believer nodes and maintains a believer node list. A source will send data to the destination only through the believer nodes. By incorporating this method, we avoid routing the data packets through malicious nodes. Our proposed scheme was analysed by using the ns2 simulations.

Key terms:
Pervasive Network, autonomous node, malicious node, ad-hoc networks

I. INTRODUCTION

A pervasive network consists of mobile nodes which are arranged independently in the environment and also they change their position dynamically. The best examples of pervasive network are MANET, WMN and VANET. The Mobile ad-Hoc Network (MANET) consists of mobile nodes which are arranged autonomously in the network environment. The nodes in MANET dynamically change its position because the topology of the network changes frequently. It is very difficult to provide the reliable routing in MANET. The application of pervasive network includes Military application, Road safety system and some critical application. So, we need to provide security while transmitting the data between the nodes. Several schemes exist that provide security in dynamic environment. However, straight forward preventive schemes. They were providing security after some malicious events occurs. In our proposed scheme we are going to route the data packets through the trustable nodes only. For that, we should make a believer list before the communication starts.

1.1 Challenges and issues:

The security challenge faced in pervasive network because of the weak link between the nodes and it includes the following:

- As the nodes are distributed in the wireless medium, it can communicate by making use of signal propagation through air medium. So, it is easy to faucet.
- The nodes present in the pervasive environment are resource limited. So, it requires proficient schemes with less overhead.
- Due to its dynamic nature, the self organizing, self healing algorithm is required to tolerate the security attacks.
- The pervasive network is vulnerable to denial of service attack.

The attacks that occur in pervasive network are broadly classified into two: Passive and Active attacks. Eavesdropping falls into the category of passive attack. In this type of attack, the intruder captures the data while it is transmitted. On the other hand in the active attacks, the malicious node misleads the other nodes that create a negative impact on the data communication.

1.2 Objective

In this paper, we propose a new efficient routing technology with security to achieve communication in pervasive network. The name of our proposed scheme is Believer based protected and efficient routing. The name itself explains that, the main goal of our proposed scheme is to provide secure routing (i.e., the source node sends its data through its believer nodes that have high energy and through those closer to the destination). This scheme protects the network against several attacks like route mislead, traffic analysis attack. Our proposed scheme

Manuscript received June 5, 2014
Manuscript revised June 20, 2014

provides attacks prevention in pervasive network in an efficient way and sustains the network security with no need of any central control.

1.3 Overview

The Believer based protected and efficient routing (BBPER) scheme accomplishes the network with believer nodes in the following way. The BBPER has five major steps to establish a secure routing in the pervasive environment. They are, distribute the cryptographic key among the network, send the puzzle to its neighbor, evaluate the puzzle reply, Make list of believers, Route packets through believer nodes.

Our proposed scheme provides the authentication between the nodes by a sending puzzle to its neighbor. The nodes which have the initially loaded cryptographic key can solve that puzzle. The nodes that efficiently solve the puzzle are included in the list of believers. The nodes that fail to solve the puzzle or those that provide incorrect solutions are added to the malicious node list.

When the node wants to route the data packets, it broadcasts the route request to its neighbor believer node. Each node forwards the route request only when the sender node is not in the malicious node list. When receiving the route reply message, the source node evaluates the route by making the comparison with its believer list. The quality of the route is evaluated by analyzing the capacity and the data rate of the nodes present in the route received. After that, the source node routes their data packets through that selected route.

II. Related works

This section describes the previous work done regarding secure routing in pervasive network. The security routing protocols mainly aimed to provide authentication, Access control and confidentiality. Still there is a gap in secure routing in the context of pervasive networks.

The routing algorithm provides the route dynamically whenever the source requires the route to reach different destination. The routing algorithm of pervasive network considers the dynamic environment of pervasive network. So, it detects the route only at the time of receiving route request message. Adhoc On demand Routing protocol (AODV), Dynamic Source Routing (DSR) and Destination sequenced distance vector (DSDV) are the conformist routing protocols of MANET [7], [8] & [10]. These routing protocols did not endow with security and prone to attacks caused by malicious node moves across the network.

Several secure routing schemes have been proposed in pervasive environment. Some of them includes secure maximal lifetime routing (SecMLR) which provides secure route and also it considers the lifetime of the network. But it does not provide security before requesting for routes. So, there is a chance of misrouting to the route request packets. Because of this process, the source node may receive insecure route as the route reply.

One of the major attacks in the dynamic environment is intrusion present in the network. This kind of attack is considered in the Sec AODV [4] routing mechanism for ad-Hoc network. This scheme uses the hash chain algorithm and digital signature to provide the security. It is a resistance to hop count modification attack. But it does not provide hop by hop authentication.

Authenticate routing for Ad-Hoc networks (ARAN) [3] which uses the digital signatures and cryptographic certificates to provide authentication. The routing messages can be authenticated, so that the authenticated nodes can only participate in the transmission in between source and destination. But it has one major problem as computation overhead. Because of that the routing performance will be declined in the form of latency in route discovery.

Feedback based secure routing protocol (FBSRP) [1] which uses the feedback information from its neighbor to know about the current status of the network. The feedback message is authenticated with one way hash chain algorithm. The feedback message is included in the MAC layer acknowledgement frame to avoid network congestion. But one major drawback in this scheme is it is vulnerable to replication attack.

III. ROUTING IN PERVASIVE NETWORK

There are several protocols available to discover the end to end route between the source and destination in Pervasive network environment. The routing protocols which are used by MANETs can also be applicable for pervasive network. Some of them include AODV, DSDV, DSR, etc.

In AODV [2] the node which requires for connection with another node broadcasts a Route Request (RREQ) packet. The nodes which all receive this RREQ check that whether it has the route to the specified destination or not. If it is, it will send the Route Response (RREP) back to the source. Otherwise, it will forward the RREQ until it reach the destination. If any error occurs in the route, the Routing error (RERR) will send back to the source node and then repeat the same process to find the new route to reach the destination.

Direct sequence distance vector routing protocol (DSDV) [6] is a table driven routing protocol. This protocol mainly considers the routing loop problem. Sequence number is one of the entries in the routing table. The sequence numbers are generated by the destination. Based on the sequence number the DSDV selects the route. But the DSDV requires regular updates of its routing table.

Dynamic source routing (DSR) [5] is a wireless mesh network routing protocol and also it is an on-demand routing protocol. It uses source routing as an alternative of relying on each intermediate node for its routing table. This makes sure that all the routing information is available at mobile nodes. It should be continually updated.DSR can find out the route in WMN by two phases which includes route discovery and route maintenance.

IV. ATTACKS IN PERVASIVE NETWORK

The pervasive network is vulnerable to the following attacks, Wormhole attack, clone attack, Mislead routing attack, flooding attack, Denial of service attack, Sybil attack.

4.1 Wormhole attack

Wormhole attack is a relay-based attack that can disrupt the routing protocol and therefore disrupt or breakdown a network and this is the reason why the attacks are serious. We can use 4 steps to explain about a general wormhole attack.

- An attacker has two trusted nodes (or two colluded attackers each has one node) in two different locations of a network with a direct link between the two nodes.
- The attacker records packets at one location of a network.
- The attacker then tunnels the recorded packets to a different location.
- The attacker re-transmits those packets back into the network location from step 1.

4.2 Clone attack

Clone attack is otherwise called as replication attack. In this kind of attack, the attacker compromises the node present in the network to capture the properties of the node and then it will introduce node with same characteristics in the network environment. So other nodes in the network cannot identify that node in the network. So, the nodes may misroute the data through this replica node. This may affect the communication in terms of confidentiality and also unreliability.

4.3 Mislead routing attack

By spoofing and altering the route reply messages the attackers may cause routing loops and may lead to redirect the network traffic and may lead to end-to-end delay etc. The routing state corruption may occur in the network. So, the nodes cannot send the data to its destination within a time. The data may not reach the destination because of routing state corruption.

4.4 Flooding attack

The intruder node present in the network frequently sends the unwanted message to its neighbors. So that node cannot perform its function properly due to overhead.

4.5 Denial of service attack

Denial of service attack attempts to make the resources unavailable to the system. It is an explicit attempt by attackers to prevent legitimate users of a service from using that particular service. Generally there are two common forms of DoS attacks: those that crash services and those that flood services.

4.6 Sybil attack

Sybil attack is the one in which the reputation system is subverted by the large no of foraging nodes. The malicious node may overhear the communication and slow down the process of reputation system.
All of the above are familiar attacks which can affect the performance of the pervasive network. But, if we provide secure routing, that way we can prevent these kinds of attacks from occurring in the system.

V. METHODOLOGY OF PROPOSED WORK:

In this section, we discuss our proposed scheme in detail. We start with the list of terms used in our proposed scheme. This is followed by the detail explanation of the proposed scheme.
List of terms used:

5.1 Believer List (BL)

This is a list which contains the trustable node in the network. Each and every node in the network should maintain this list in its data structure. Each node maintains which are its neighbors are believer node.

5.2 Malicious node list: (ML)

This list should also be maintained by each node in the network. The nodes which are not participated in the believer list enter into malicious node list. All suspicious nodes present in the network also present in the malicious node list.

5.3 Believer route request (BRREQ)

When the source node sent the data to its destination, it would broadcast the BRREQ message to its believer nodes.

The believer nodes again forward the request if the sender node is not present in their malicious node list.

5.4 Evaluate route (ER)

After receiving the route reply from its destination, the source node evaluates the route and chooses the best route based on the capacity of the intermediate nodes present in the network.

5.5 Believer based protective and efficient scheme

The processes involved in the BBPER scheme are subdivided into the following modules. They are,

- Distribute the cryptographic key among the network
- Send the puzzle to its neighbor
- Make list of believers
- Route packets through believer nodes

5.6 Distribute the cryptographic key among the network

Initially, all the nodes distributed in the pervasive environment are preloaded with the randomly generated cryptographic key. That key is used to evaluate the node, whether it can be believable or not. The nodes used that key to answer the puzzle received from its neighbors.

5.7 Send the puzzle to its neighbor

Before the transmission starts, each and every node should create its believer node list. For that, it sends the puzzle message to its entire neighbor. The puzzle is making by the node by using the following formula

$$\text{Puzzle} = C^d \bmod CK$$

Where,
C and d is the randomly generated number CK is the cryptographic key assigned to each node The node which has that key can reply correctly to that puzzle. By evaluating the puzzle reply the node which goes to make the believer list will enter the believer node into the believer list.

5.8 Make list of believers

Each and every node should maintain believer node list in its data structure. So all the nodes have to send the puzzles to its neighbor and have to analyse the puzzle reply to select the believer nodes. The nodes which reply correctly to the puzzle sending node can only enter into the believer node List.

5.9 Route data through believer nodes

After making the believer node list and the malicious node list the nodes in the pervasive network can communicate with each other. The source node sends the BRREQ to each of its neighbors present in its believer node list. Then all believer nodes forward the BRREQ to its believer nodes until it reach the destination. The destination sends the BRREP message back to the source. The source node selects the best route among this by analyzing the capacity of the intermediate node present in the route. Finally, the source node route the data packets through its believer nodes. So, we can prevent the network from several attacks.

VI. RESULTS AND DISCUSSION

The proposed scheme is evaluated by using the NS-2 simulator. In our simulation we are connecting the nodes in MANET environment. In this simulation we placed 21 nodes randomly. For every node energy and their packets received by sink node are calculated. Each node sends puzzle reply to their sink node. If a node does not complete the puzzle correctly, it is declared as malicious and isolated from network. But other protocols (TMR an MTMR) rely on the trust of a node. They take time to come to a conclusion that a particular node is malicious or not. As we increase the number of nodes, more malicious nodes are detected by BBPER as more friends sharing could be done. Nodes which have completed puzzle finds place in the believer node list. A node which does not complete the challenge is shifted to the malicious node list, which is a list, containing information about the malicious nodes. It signifies mis-trust on the node, and it is not used subsequently in the routing process.
As less-packets are routed through the malicious nodes, it implies that BBPER protocol has better security characteristics. This is due to efficient detection of malicious nodes. As compared to other protocol FBSRP, it does not route anything to malicious nodes. Nevertheless, the other protocols detect malicious nodes after some delay and as a result, suffer more packet loss. As we increase the number of nodes or the mobility, more number of packets is transmitted through malicious nodes. This has been shown in Figure.1.This happens because more packets need to be routed to make new friends each time a node moves out of the range of its neighbor.

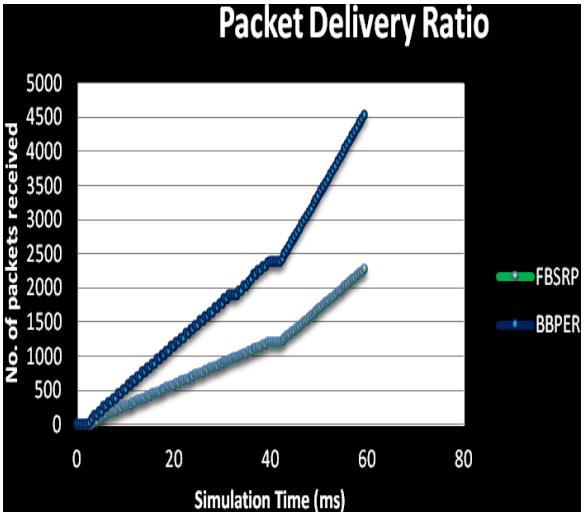

Figure.1 Packet received ratio graph of the proposed scheme BBPER

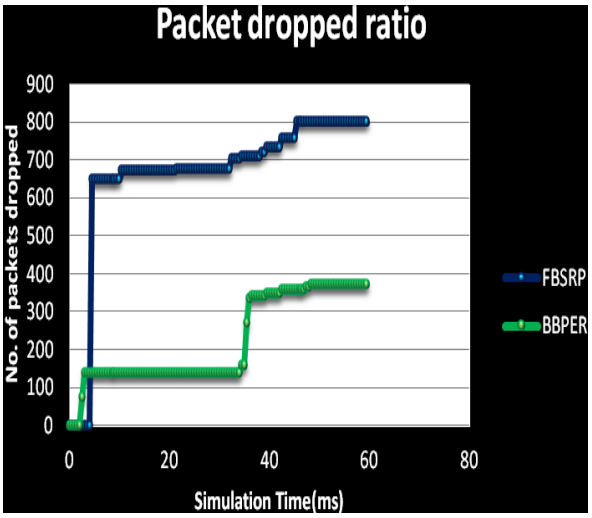

Figure.2 Packet dropped ratio graph for the proposed scheme BBPER

We can see that the packet drop is minimal in BBPER from figure.2; as it efficiently discards routes containing malicious nodes. The other multipath routing protocols drop a large number of packets as they route through greater number of nodes and thus increasing the chances of routing data through malicious nodes. As we increase the number of nodes or even the mobility, it is found that the number of packet drop increases. As believer node list is difficult to maintain in a highly mobile environment, it is seen that there is a sharp increase in the packet drop of BBPER, but even then the BBPER protocol performs better than the other protocols.

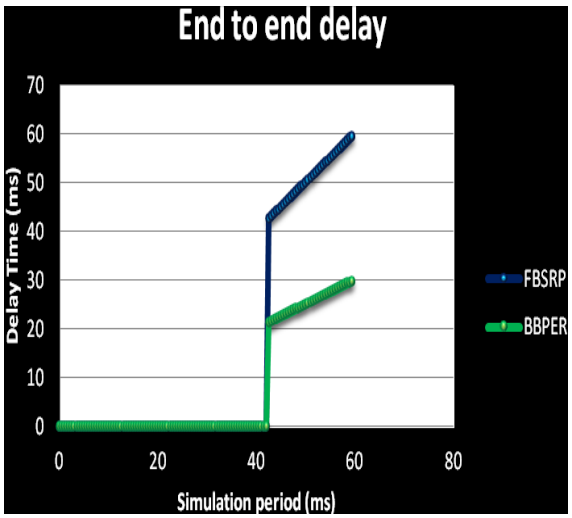

Figure.3 End to end delay analysis for the proposed scheme BBPER

The delay occurs in the network is calculated by lastPacket_ command in NS2 simulator. The delay for both the existing and the proposed system has been calculated and these parameters have been plotted as a graph which is shown in Figure.3. Lower value of delay indicates that the better performance of the proposed scheme. From Figure.3, it has been proved that, the proposed scheme outperforms than the existing one.

VII. CONCLUSION

After a logical analysis and extensive simulation of the BBPER algorithm under diverse scenarios, we come to the conclusion that it offers robust scheme to afford security for mobile ad hoc networks and performs better than the trust based protocols from which it was compared. The network has to bear a lot less overhead as compared to other secure routing schemes, due to the absence of the need of promiscuous mode in the mobile nodes. The friends sharing scheme turns out to be an efficient mechanism to spread information about trusted nodes effectively in the system. Since the algorithm does not rely on any scheme to spread information about misbehaving nodes, there are no chances of grudge wars taking place in the network. The maliciousness of a node is on the sole discretion of a certain node, which it determines through challenges. Challenges turn out to be an efficient mechanism to authenticate nodes because the malicious nodes cannot differentiate between a packet that is meant for a challenge and the one meant for normal data routing. This provides an inherent security to the network and the malicious nodes are easily exposed. This on the other hand reduces overheads and hence reduces the chances of unsecured routing through faulty nodes. Due to these

challenges, the BBPER protocol works much better and provides more security than the other multipath routing protocols. Future work can be done on how this scheme can be implemented combined with some of the general protocols that come under Flat Routing Protocol, Pro-Active / Table Driven routing Protocols, Hierarchical Routing protocol and Geographical Routing protocols [9].

REFERENCES:

[1] Zhen Cao, Jianbin Hu, Zhong Chen, Maoxing Xu, Xia Zhou, "FBSR: Feedback based Secure Routing Protocol for Wireless Sensor Networks", J. PERVASIVE COMPUT. & COMM.

[2] C. Perkins, E. Belding-Royer, and S. Das. Ad hoc On-Demand Distance Vector (AODV) Routing. RFC 3561 (Experimental), July 2003.

[3] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E.-M. Belding-Royer. A Secure Routing Protocol for Ad Hoc Networks. In Proceedings of International Conference on Network Protocols (ICNP), pages 78–87, Paris, France, November 2002.

[4] J. Hubaux, L. Buttyan, and S. Capkun. The Quest for Security in Mobile Ad Hoc Networks. In Proceedings of the 2nd ACM International Symposium on Mobile and Ad Hoc Networking & Computing (MobiHoc 2001), pages 146–155, Long Beach,CA, USA, October 2001.

[5] D. B. Johnson and D. A. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. In Tomasz Imielinski and Hank Korth, editors, Mobile Computing,chapter 5, pages 153–181. Kluwer Academic Publishers, 1996.

[6] C.E. Perkins & P. Bhagwat, "Highly Dynamic Destination Sequence-Vector Routing (DSDV) for Mobile Computers", *Computer Communication Review, 24*(4), 1994,234-244.

[7] V. P. Patil, K.T.Patil, A. R. Kharade & D. D.Gote, "Performance Enhancement of Reactive on Demand Routing Protocol in Wireless Ad Hoc Network", International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) Vol-1, Issue-4, 2012

[8] A. Dhatrak, A. Deshmukh and R. Dhadge, "Modified AODV Protocols: A Survey" 2nd National Conference on Information and Communication Technology (NCICT) 2011 Procs published in International Journal of Computer Applications (IJCA)

[9] P. Sharma, A. Kalia and J. Thakur, "Performance Analysis Of Aodv, Dsr And Dsdv Routing Protocols In Mobilead-Hoc Network (Manet)", Journal of Information Systems and Communication", Vol. 3, 2012, pp.-322-326

[10] N. S. Mohamad Usop, A. Abdullah, and A. F. Abidin," Performance Evaluation of AODV, DSDV & DSR Routing Protocol in Grid Environment," International Journal of Computer Science and Network Security (IJCSNS), Vol.9 No.7, July 2009