Fuzzy Based Secure Enhanced Reactive Routing Protocol Using Bayesian Probability in Manet

M.Deepa¹, Dr. P. Krishna Priya²

¹ Ph.D. Scholar, Department of Computer Applications, Coimbatore Institute of Management and Technology, Tamil Nadu, India.
² Director, Department of Computer Applications, Coimbatore Institute of Management and Technology, Tamil Nadu, India.
E-Mail: deepshini21@gmail.com, krishnapriya.p@kgcas.com

Abstract: The proposed protocol Secure AODV – ESBF (Adhoc on Demand Distance Vector based on Energy level and Signal Strength Implementing Bayesian Probability and Fuzzy Logic) is a modification of existing dynamic protocol AODV. In AODV protocol Hop count is considered as metric for the process of route selection. Whereas in proposed protocol route is selected based on Energy Level of nodes and Signal strength that exist between them. Since Energy level and signal strength act as two factors that determine effectiveness of the route, Bayesian probability is implemented to select optimized path in a more accurate and efficient manner. In selected optimal paths the RREQ will be forwarded and reach destination. As need for efficiency of the routing, the security of the routing is also of immense importance. The security to protocol is implemented in two phases. In first phase, security is provided by preventing from selecting malicious node as the neighbor node and simultaneously preventing from RREQ forwarded to the malicious node by eliminating it. The insecure nodes are eliminated and efficient neighbors are selected and RREQ is forwarded to limited neighboring nodes based on energy level of nodes and signal strength of links implementing the Bayesian probability. The second phase of security is implied by implementing the Two Fish cryptography algorithm during process of data transmission from source node to the destination. To further improve the efficiency of Bayesian implemented modified secure AODV protocol in this work, the fuzzy logic is implemented. Fuzzy logic is implemented in destination node in process of selecting more stable path from routes forwarded from source node. The simulations are performed in NS2 network simulator and results proves that the proposed protocol is efficient compared to the AODV protocol and other earlier modifications of AODV protocol.

Keywords: Mobile Adhoc Network (MANET), Network Simulator (NS 2), Bayesian Probability, Two Fish Algorithm, Fuzzy Logic

I. INTRODUCTION

The infrastructureless Wireless network is denoted by the term MANET (Mobile Adhoc Networks) [1]. This network is based on the hop by hop transmission of packets. If the destination available within the radio range of a node then the transmission of packet occurs directly in single hop and in case of destination present beyond the radio range then the neighbor nodes acts as the intermediate nodes and transmit data towards the destination node. In this adhoc dynamic network each node performs the function of the router. Routing plays a major role in the adhoc arbitrary network. MANET routing protocols are widely classified as proactive, reactive and hybrid protocols [2].
In case of proactive routing protocols the routes are predetermined, in reactive routing protocol the routes are obtained on demand and in case of the hybrid the routes are predetermined to certain extent and beyond that the routes are assigned on demand. Each protocol has unique features and its works efficiently in suitable network environments [3]. The reactive routing protocol performs more efficiently in case of high mobility and dense network [4]. The AODV is an efficient reactive routing protocol for MANET [5]. The major limitation of this AODV protocol is the frequent occurrence of link failure caused due to power failure of the node or loss of signal strength resulting in reduced throughput and packet delivery ratio and increased end to end delay and control overhead [6][7]. In this work an enhanced AODV routing protocol modified using Bayesian probability and secured implementing two fish algorithm in my previous work is further improved implementing fuzzy logic.

Hop count alone is used as metric for route selection in AODV protocol. In the prior work the node power level and signal strength are used as the metric for route selection. Bayesian probability is used to make optimal decision efficiency based on these two parameters efficiently. Security features are added to eliminate the malicious node and also two fish algorithm is used for secure transmission of data from the source to destination. In this proposed protocol secure AODV-ESBF the efficiency of the optimized secure AODV protocol is further improved by using the Fuzzy logic. The of the proposed protocol AODV-ESBF is evaluated by performing simulations and the obtained result is compared with the results of AODV protocol and the previous works AODV-ESB and Secure AODV-ESB protocol. The performance results shows that the current proposed work is comparatively more efficient than the previous works.

The rest of the paper is organized as follows. A review of the routing protocols in MANET and existing previous modifications of AODV protocols related to this work are discussed in detail in section II. Discussion about the AODV protocol details and its working methodology is briefly discussed in section III. The enhanced secure AODV-ESBF protocol structure and methodology is explained in section IV. The section V presents the simulations results obtained from different scenario performed using proposed protocol with fuzzy in NS2 and comparative results obtained for the AODV protocol and the earlier modifications are also presented. The conclusion is presented in the section VI.

II. RELATED WORK

Routing plays a major role in adhoc networks. The AODV reactive routing protocol using the Bayesian probability provides a better performance [8]. Security is also a major requirement of the routing protocol for the secure transmission of data [9].

The author in paper [10], proposes a new protocol fuzzy logic stable-backbone-based multipath routing protocol (FLSBMRP), which initially performs node selection using the fuzzy logic. Then constructs multiple paths between the selected nodes and if any node fails alternate path is selected for transmitting data.

In [11], the author has presented a protocol using the soft computing technique fuzzy logic, which attains a reduced control overhead and requires less storage. The three input values used as input values by this protocol are signal power, mobility, and delay.

In [12], the paper proposed by the author utilize crosslayer based multicast. The parameters suggested for better performance by taking battery over, source node as input values for fuzzification. To provide a better performance.
In [13], the author has taken the signal strength, Mobility model, packet forwarding ratio and bandwidth as the input parameters for the fuzzification process. Gaussians function

In [14], the author has presented a new protocol Fuzzy Trust based on Bayesian Statistical Model (FT_AOMDV), a modified multipath AODV protocol AOMDV provides a better performance than the AODV protocol. This protocol initially verifies the trust worthiness of the neighbor and routing process takes place between trusted neighbors. Trust value and RSSI are taken as input for fuzzification. Various in the proposed work from the trusted neighbors, the nodes for active path are selected based on the energy level and signal strength. Reliability rate is obtained as output of defuzzification in FT_AOMDV, whereas reliability rate is obtained using the Bayesian probability in the proposed work.

III. AODV ROUTING PROTOCOL

The AODV protocol is an on demand efficient reactive routing protocol in MANET. The AODV protocol is an advancement of the DSDV protocol. Bellman-ford is the base route mechanism of the DSDV protocol. AODV routing protocol overcomes the drawbacks of the DSDV protocol. In AODV routing process the routes are discovered only on demand. when the source requires to transmit a packet to destination node, the RREQ packets are broadcasted. If the destination node is within the radio range of the source node the packets are directly transmitted, otherwise the packets are transmitted to the destination through the intermediate node.

In the AODV protocol the routing information are maintained only for the nodes in the active path. In this protocol the packets are transmitted hop by hop. The routing process in this protocol takes place in two phases. The route discovery phase and route maintenance phase. When a path is required for transmission the route discovery is initiated and path details are maintained only for the nodes that lie in the active path.

During the route discovery process the RREQ packets are broadcasted to all the neighboring nodes. If the destination node is within the radio range of the source node the packet is directly transmitted otherwise the packets are further transmitted to their neighboring node. Packets reach the destination passing through the intermediate nodes.

A. AODV PROTOCOL USING BAYESIAN PROBABILITY: AODV-ESB

The AODV protocol uses hop count alone as the metric for path selection and faces frequent link failure caused by the power failure of the node and loss of signal strength. This major drawback of the AODV protocol has been overcome in the AODV-ESB protocol. It utilizes the power level of the node and the signal strength that exist between two nodes as the metric for route selection. When two parameters exist and based on both if the decision is to be taken then Bayesian probability can be utilized. It reduces the number of RREQ and control overheads broadcasted. The RREQ packet forwarded to the selected neighboring nodes optimal paths are formed towards the destination.
IV. ENHANCED AODV PROTOCOL USING FUZZY LOGIC

Fuzzy logic is an approach to computing based on degrees of truth rather than fixed and exact values. Traditional logic theory deals with binary set that have two-valued logic: true or false, whereas fuzzy logic may have a truth value that ranges in degrees.

The proposed work secure AODV-ESBF, an enhanced routing protocol for MANET is an advancement of the AODV protocol, which is modified in four different levels. Four different phases of optimization of this proposed protocol are

PHASE 1: Elimination of the malicious node
PHASE 2: Route selection using Bayesian Probability
PHASE 3: Optimal route selection by destination node Using fuzzy logic.
PHASE 4: Implementing security using Two Fish Algorithm

This proposed protocol mainly target on the challenges faced by the MANET routing protocols and the attacks that targeted on them. Problems targeted to solve are the frequent link breaks due to node power failure and loss of signal strength, the attack of the malicious nodes and attack on data during data transmission by the intruders. Initially from the starting of the simulation process the network is monitored. The node behavior is observed, if any node behavior is found to vary from the normal behavior that particular node is identified as the malicious node and eliminated.

Fig.1 General Structure of proposed secure AODV-ESBF Protocol
Each node in the network is surrounded with good neighbors after the elimination of the malicious node. Next process followed is the optimal route selection, considering the node power level and the signal strength as metric. Since two parameters, Bayesian probability is used to find the combined optimal values for node, based on which the neighbor selection takes place and the RREQ packets are forwarded through intermediate nodes towards the destination node. Now among the optimal routes reaching the destination node, the most reliable path is selected by the destination node by using the fuzzy logic. As the route selection process is completed the data transmission starts from the source node. Security is a major factor to be considered. For secure transmission of data, the data is encrypted in the source node and forwarded through the intermediate nodes towards the destination node and the data on reaching the destination node gets decrypted. This security feature is implemented using the two fish algorithm.

A. PHASE 1: ELIMINATION OF THE MALICIOUS NODE

Monitoring the network and collecting the data is the initial process of the protocol in this phase each node in this network maintains link table and a result table. RREQ, RREP and RERR values are stored in the link table and control packet counts, loss packets and percentage of packets received are stored in the result table. While starting the process both the tables are updated in frequent intervals. In each interval the average value is taken and the tables are updated for each node. In the earlier stage the nodes character reputation is based on these values.

The presence of any attack on node is verified by validating its link table. Here the updation of link table, takes place with the values of the probability estimation made on the network link values. Each time the proposition values for the links are updated by the node. If any node exists without proposition being computed, it indicates the presence of attacker. Once presence of attacker is identified, the attacker is identified by policy. Using the result table the result deprivation is estimated. Each node conveys the self-assurance of its neighbors. As the self-assurance is obtained normal node eliminates the harmful node from the network activities. On eliminating the harmful node the nearby good node is supposed to transmit data instead of the harmful node. In case of absence of good node near the eliminated harmful node then some other good node is purposely moved to attacker’s position.

B. PHASE 2: ROUTE SELECTION USING BAYESIAN PROBABILITY

The route discovery process is initiated by selecting the optimal path on the basis of energy level of the node and the signal strength of the link. The case of loss of parameters energy level and signal strength is the main cause for the link breaks in MANET. To overcome these problems, both these parameters are considered as the metric for route selection. Since two piece of information is to be considered, Bayesian probability is used to estimate a value based on these two matrices. Implementing Bayesian probability in the protocol is to reduce number of broadcast, resulting in reduced control messages and save bandwidth and node power.

C. PHASE 3: OPTIMAL ROUTE SELECTION BY DESTINATION NODE USING FUZZY LOGIC

Fuzzy logic is widely implied for various applications for the efficient performance. In the proposed protocol the fuzzy logic is implied in the later phase only. Implying the Bayesian probability only the stable neighbors lie in the forwarded path. Among the arrived path from the source node to the destination node, the most reliable path is selected by the destination node by using the fuzzy logic and in the selected path the RREP is unicasted towards the source node and the data will be forwarded from the source node to the destination.
Fuzzification is executed in the destination to get an optimal path. It converts numerical data into fuzzy member sets. The input of the member sets are hop count, energy level of the node, neighbors and queue size. It identifies all possible combination of fuzzy member sets and proceeds with rule composition. Fuzzy rules are created based on the rule inference to get the best value path. After obtaining the reliable best optimal path defuzzification is done to get final value in order to construct path. Each node initially shares all the above said parameters along with the routing messages. Destination collects all details and executes fuzzy to get optimized values.

**D. PHASE 4: IMPLEMENTING SECURITY USING TWO FISH ALGORITHM**

A major requirement in network routing is the secure data transmission. Two fish algorithm is an efficient cryptography algorithm. It's one of the top five finalist of the AES algorithm contest. It’s a 128 bit block cipher. The cipher is a 16 round Feistel network. Two fish algorithm is successor of the Blow fish algorithm. In the proposed protocol the data is encrypted using the two fish algorithm in source node and the encrypted data is transmitted through the intermediate node and reaches the destination node in the most reliable path. On reaching the destination the data is decrypted using the two fish algorithm again.

**V. SIMULATION MODEL**

The NS2 simulator is used for the purpose of evaluating the proposed protocol Secure AODV-ESBF. The efficiency of the protocol is analyzed by varying the input values and performing the simulations under different scenario. The performance of the protocol is monitored under varying network size, different interval and various packet sizes.

**EVALUATION METRICS**

The protocols are observed during the simulation under different circumstances and their efficiency is evaluated based on certain metrics. The Throughput of the network and packet delivery ratio is observed. The end to end delay occurred during transmission of the packet from source to destination and the control overhead generated during the simulation process are the metrics considered for evaluating the protocol in this current work.

**B. SIMULATION ENVIRONMENT**

In simulation, three scenarios are performed to analyze the performance of the proposed protocol. In the first scenario the number of nodes is varied from 50 to 100 and performance is evaluated. In the second scenario the performance is evaluated by varying the interval. The third scenario analyses by varying the packetsize. The Table 1 contains the parameters set for this simulation.

<table>
<thead>
<tr>
<th>S.No</th>
<th>Parameter Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Network Size</td>
<td>1000 m x 1000 m</td>
</tr>
<tr>
<td>2</td>
<td>Number of Nodes</td>
<td>50, 60, 70, 80, 90, 100</td>
</tr>
<tr>
<td>3</td>
<td>Simulation Time</td>
<td>200 Sec</td>
</tr>
<tr>
<td>4</td>
<td>Antenna Model</td>
<td>Omni antenna</td>
</tr>
<tr>
<td>5</td>
<td>Radio Propagation</td>
<td>Two ray ground</td>
</tr>
<tr>
<td>6</td>
<td>Channel Type</td>
<td>Wireless Channel</td>
</tr>
<tr>
<td>7</td>
<td>Pause Time</td>
<td>0.1 sec</td>
</tr>
<tr>
<td>8</td>
<td>Packet Size</td>
<td>1000 bytes</td>
</tr>
<tr>
<td>9</td>
<td>Traffic Type</td>
<td>Constant Bitrate(CBR)</td>
</tr>
<tr>
<td>10</td>
<td>Data Transmission</td>
<td>UDP</td>
</tr>
<tr>
<td>11</td>
<td>MAC Protocol</td>
<td>IEEE 802.11</td>
</tr>
<tr>
<td>12</td>
<td>Routing Protocol</td>
<td>AODV</td>
</tr>
</tbody>
</table>
C. SIMULATION RESULTS

The proposed system is simulated using NS2 simulator and the results have been obtained. The simulations are performed as discussed in the section IV. The simulations results obtained for the proposed protocol are compared with the results obtained from simulations carried on using the protocols obtained from the previous works. The results clearly depicts that the secure AODV-ESBF protocol is more efficient than the other protocols Secure AODV- ESB, AODV-ESB and the existing AODV protocol.

Scenario I: Evaluation performed by varying the number of nodes

The throughput obtained for secure AODV – ESBF, secure AODV – ESB, AODV – ESB and AODV protocol, by varying the number of nodes is depicted in Fig 2. The comparison results show that the proposed protocol in this work Secure AODV- ESBF provides a higher throughput compared to the other protocols throughout the simulation process. The packet delivery ratio with the varying number of nodes seems to remain above 95% while the AODV has packet delivery ratio of 85 %other earlier modifications attains 90% to 95% packet delivery ratio. Fig 3. Shows that analyzing the packet delivery ratio, Similar to the throughput the packet delivery ratio of the proposed protocol is also higher than the original and earlier modifications of the AODV protocol. From Fig 4 it's clear that the secure AODV-ESBF protocol faces approximately 0.6 sec lesser end to end delay compared to that of AODV protocol. Fig 5. Shows that with increase in number of nodes there is increase in control overhead and compared to AODV protocol the proposed protocol has lesser control overhead. But still the proposed Protocol has greater overhead than its other earlier modifications.

![Fig. 2: Variation of Throughput with network size](image)

![Fig.3: Variation of PDR with network size](image)
Scenario II: Evaluation performed over different Interval

Fig 6. Depicts that with increase in interval there is an increase in throughput of all the protocols gradually and throughout the simulation process, but it also maintains a lower end to end delay compared to AODV protocol and other earlier modification protocols. Fig 7. Shows that variation in interval does not show much variation in packet delivery ratio. The proposed protocol constantly provides a higher packet delivery ratio compared to AODV protocol and other earlier modifications. Fig 8. clearly shows that proposed protocol has increase and decrease of end to end delay throughout the simulation process, but it also maintains a lower end to end delay compared to the AODV and AODV-ESB protocol. End to end delay of secure AODV-ESB and secure AODV-ESBF are almost similar. Fig 9 shows that AODV-ESB has much lower overhead compared to the AODV protocol, but the secure AODV-ESB and secure AODV-ESBF generates a moderate range of control overheads.
Scenario III: Evaluation performed by varying the Packet size

Fig 10. Depicts that the secure AODV-ESB protocol has higher throughput than the secure AODV-ESBF protocol, while the AODV and AODV-ESB protocols has lesser throughput than the proposed protocol. Fig 11. Shows that the packet delivery ratio of the proposed protocol is higher than the AODV and other earlier modification protocols. The secure AODV-ESBF protocol maintains a packet delivery ratio above 95% throughout the simulation with varying packet size, while other compared protocols attain below 94%. The end to end delay of the proposed protocol remains lesser than the other compared protocols.
The variation in only minimum compared to the Secure AODV-ESB protocol. Fig 12. Shows that the control overhead for the AODV-ESB protocol is lesser compared to other protocols. While the security features are added the control overheads also have increased. But the variation in packet size does not have any impact on the generation of control overheads. Adding fuzzy to the secure AODV-ESB protocol has reduced the generation of control overhead.

![Variation of Throughput with Packet size](image1)

![Variation of Packet delivery ratio with Packet size](image2)

![Variation of end to end delay with Packet size](image3)

![Variation of control overhead with Packet Size](image4)
VI. CONCLUSION

The proposed protocol secure AODV-ESBF is a modification of efficient reactive AODV routing protocol. It overcomes the problem of frequent link failure occurred in AODV protocol due to the power failure of node and loss of signal strength. Bayesian probability is used to overcome this problem by detecting the chances of node failure and avoiding occurrence of frequent link breaks. Implementing Two Fish algorithm and security features provides a secure transmission of data across the network. Modification of the protocol using fuzzy logic improves the efficiency of the protocol and provides a better result. Thus the simulation results clearly depicts that the proposed protocol Secure AODV-ESBF, performs better compared to the AODV protocol and the other earlier modifications of the AODV protocol.

REFERENCES

[1] Lu Han, “Wireless Ad-hoc Networks”, Oct 8, 2004