ABSTRACT

Mobile Adhoc Networks (MANET) is a heterogeneous self-configuring networks that changes topology often. Due to mobility nature of wireless nodes, routing information needs to be frequently updated. As nodes are wireless in nature, there exists enormous security threats that disturb the deployment and maintenance of MANET. To alleviate such problems, secure agent based multicast routing protocol for wireless network is proposed which is an extension of existing AQMRA. Group communications require stringent QoS parameters and they have to be kept in rigorous bound. In the proposed work Secure ANFIS based QoS Multicast Routing Agent (Secure AQMRA). QoS input parameters namely node speed, link delay, residual power, packet loss, bandwidth, link utilization are optimized to achieve better scalability. Secure agents are configured in each and every node in the network. This protocol guarantees the security, scalability and high reliability of an established route. The proposed Secure AQMRA protocol performs better than the existing AQMRA protocol in terms of end to end delay, control overhead and Packet Delivery Ratio.

KEYWORDS—MANET, Neighbor discovery, Multi-agent, Secure Routing, Neuro Fuzzy, Optimization, QoS.

I. INTRODUCTION

Security and efficient routing are the two major challenging metrics that needs to be addressed. In Multihop routing, packets are transmitted between one or more intermediate nodes which requires frequent updating of routing table. So, there exists a chance of packets to be dropped or delay in packets which ultimately affects the overall performance of the networks. The wireless behavior of mobile nodes helps the eavesdropper to steal the information and more prone to security attacks.

A. Quality of service (QoS)

QoS is the capacity of wireless network to yield best service over various technologies. QoS parameters such as Speed, bandwidth, throughput, availability, jitter are often considered to be optimized for better routing and handling scalability.

B. Fuzzy Neural Network or Neuro-Fuzzy System

A Fuzzy Neural Network[10] is a learning machine that finds the parameters of a fuzzy system by exploiting approximation techniques from neural networks. ANFIS(Adaptive-Network-based Fuzzy Inference System) is an inference system which is implemented in the framework of adaptive networks. ANFIS can develop input-output mapping in the form of fuzzy if-then rules and stipulated input-output data pairs.

The Layers used in ANFIS are

- Fuzzification
- Rules
- Normalization
- Defuzzification
- Output

Layer 1: Fuzzification

The degree of membership function is determined.

Layer 2: Rules

Computes the firing strength of the associated rule

Layer 3: Normalization

The normalized firing strength of a given rule is calculated

Layer 4: Defuzzification

The weighted consequent value of a given rule is calculated.

Layer 5: Output

Output layer consisting of single fixed node obtained by combining outputs from Layer 4.

C. Software Agents

Software agent is a computer program works in an intelligent manner. It is classified as static and mobile agent. Static agent is immovable; it just resides on its host and performs the activities on behalf of user. Mobile agent is a software program which can move from one host to another to perform the assigned task. User monitoring agent monitor the user, if any request generated, it triggers other agent to perform task or activities. Route discovering agent is a mobile agent which moves from one node to another and helps to discover the routes for data transmission. Route maintenance agent is a mobile agent which freely roams along the network path and detects the faulty link and recover. This paper is catalogued as follows. Section II briefs related works. Section III explains about the methodologies to configure the agents for improving QoS parameters. In Section IV, results are analyzed through simulation. Performance evaluation is carried over in Section V. Section VI concludes with the summary of the proposed work.

II. RELATED WORK

Ariadne et.al [1] proposed Secure On-Demand Routing Protocol for adhoc networks which relies on Symmetric Cryptography. Ariadne avoids attackers from meddle with untrusted routes and hinders many types of DOS attack. This protocol uses segment of the bandwidth along each link. But this protocol has higher overhead in terms resources and bandwidth requirements.

Yih-Chun Hu a,* ,David B. Johnson b, Adrian Perrig [2] proposed Secure Efficient Ad Hoc Distance Vector (SEAD) which is fundamental principle on DSDV protocol. SEAD make use of one-way hash chains to establish the authorship and give shares of such hash chains. This scheme suffers from network overhead due to large number of advertisement messages.

Fuzzy logic control is used in the proposed method [6] to increase the performance and reliability of the multicast routing protocols in MANET. To reduce resource usage and multiply stability, Strong and small forwarding group is obtained. Fuzzy logic is to distinguish the strong and weak nodes in the network. At regular intervals, Join query packet is relayed to bring up the routes in the network. Node receiving join query message must fuzzyfys the QoS parameters of previous node. Inference process is carried out to obtain the probability of caching. Adaptive fuzzy inference system is proposed [5] to rise the scalability of adhoc networks. Fuzzy network
consist of three layers. First Layer represents input variables. Intermediate Layer represents the fuzzy rules. Third Layer represents the output variables. Adaptive Fuzzy Inference System helps in improving the scalability by combining Fuzzy Logic Inference and Recursive Least Square Algorithm. This scheme suffers with lack of security. Quality-of-Service (QoS)-based multicast routing protocol (QoS-MR) is proposed [8] for mobile adhoc network. QoS-MR is a receiver-initiated mesh-based multicast routing protocol and can work for both stable and unstable networks. Initial broadcast message called BRQ TSPEC is sent to all the nodes in the network. Multicast Routing Table (MRT) is maintained in all nodes in the network to update the receiving BRQ TSPEC messages.

**Motivation of Proposed Work**
Due to dynamic nature of mobile nodes and restricted resources, providing desired Quality of Service is a challenging task. As nodes are wireless, there is a chance of attackers to steal and hijack the networks which ultimately degrade the quality of the service. To address this issue, we propose extensions for Secure Agent Based Multicast Routing protocol.

**III. METHODOLOGY**
This section describes the extension of ANFIS based QoS multicast routing protocol.

The following contributions were made in the proposed work.

Firstly, QoS input parameters are optimized using Adaptive Neuro based Fuzzy Inference System (ANFIS). Secure agents are configured in each and every node using SHA algorithm. Multicast administer agent (static agent) is used to forward the QoS satisfying nodes for routing. Route inventing mobile agents trace back the traversed path by marking QoS nodes. To reach the multicast receivers MAA selects the shortest path using Floyd’s algorithm. NSA algorithm is used to encrypt the data packet for transmission. Guard agent is employed for link/node failures and management of the group. This system guarantees the security, scalability and high reliability of an established route.

**Fig 1. System Architecture**

**A. Optimize membership function using ANFIS**
In Mobile Adhoc Networks, when the number of nodes increases then the performance degrades. In order to improve the scalability, the membership functions are optimized using ANFIS (Adaptive Neuro Fuzzy Inference System) scheme. ANFIS structure is based on six inputs such as Node speed, Link delay, Residual power, Packet loss, bandwidth and link utilization. Input parameters are optimized using fuzzy If Then rules. Once optimization process is completed, QoS satisfying nodes are discovered and routing takes place only through the QoS satisfying nodes. QoS unsatisfying nodes are discarded from the data transmission.

**Fuzzy If Then rules considered in this work are**

If NS is S1, LD is D1, RP is P1, PL is L1, BW is W1 and LU is U1 then

\[ f_1 = a_{11} NS + a_{12} LD + a_{13} RP + a_{14} PL + a_{15} BW + a_{16} LU + H1 \]

where NS-Node Speed, LD-Link Delay, RP-Residual Power, PL-Packet Loss, BW-Bandwidth and LU-Link Utilization. \( f_1 \) is the optimized QoS value.

**Algorithm Steps**
QoS requirements are collected from the users. The QoS parameters are optimized using Neuro-Fuzzy Model. If the QoS factor is greater than the QoS requirement, then the node is considered as QoS satisfying node.

**B. Secure agent configuration**
In this, agents are securely configured using SHA algorithm. SHA uses hash function ‘H’, accepts variable length block of data ‘M’ as input and produce fixed size hash value \( h=H(M) \). Agents used in the system are Multicast Administrator Agent(MIA), Route Inventing Agent (RIA) and Guard Agent(GA).

**Steps:**

Step 1: ANFIS Agent is used to find the QoS satisfying nodes.

Step 2: Multicast administer agent MAA (static agent) is used to forward the QoS satisfying nodes for routing.

Step 3: Route inventing agent establish the route between Source and Destination.

Step 4: MAA selects the shortest path from that route using Floyd warshall’s algorithm.

**C. Shortest Path Discovery**
From source to destination, there would be more than one path. Shortest path discovery is performed to identify the shortest path among multiple paths. This mechanism implements Floyd algorithm to improve the efficiency and thereby reduces the time complexity.

**Floyd algorithm**

Input n: Number of vertices

\[ a[0..n-1][0..n-1] \rightarrow \text{Adjacency matrix} \]

Output: Transformed Matrix that contains shortest path lengths

for \(( k = 0; k < n; k++ )\)

for \(( i = 0; i < n; i++ )\)

for \(( j = 0; j < n; j++ )\)

\[ a[i][j] = \min ( a[i][j], a[i][k] + a[k][j] ) ; \]

**D. Data Encryption using NSA**
After identifying the shortest path, data to be transmitted are encrypted for secure data transmission. Two families of highly optimized block ciphers are used for data encryption namely Simon and Speck.

RC4 algorithm is used for encryption and decryption process.

Step 1: Get the data to be encrypted along with the secret key.

Step 2: Two string arrays is created.

Step 3: Initiate one array with numbers from 0 to 255.

Step 4: Fill the other array with the selected key.

Step 6: The first array is randomized, depending on the array of key to generate the final key stream.

Step 7: The final key stream is XORed with the data to be encrypted to give cipher text.

**Algorithm:**

**Step 1: Initialization**

for \( i = 0 \) to 255 do

\[ S[i] = i; \]

\[ T[i] = K[i \text{ mod keylen}]; \]
Step 2: Initial Permutation of S
j = 0;
for i = 0 to 255 do
j = (j + S[i] + T[i]) mod 256;
Swap (S[i], S[j]);
Step 3: Stream Generation
i, j = 0
while (true)
i = (i + 1) mod 256;

IV. SIMULATION RESULTS

A. Simulation Environment
The evaluations of the protocols are carried out with the network simulator NS-2. The random way point network model is used in the simulation according to the distance X, Y, Z coordinates.

Fig 2 QoS Discovery of neighbor nodes
Initially 150 nodes are considered for simulation environment. Fig 2 shows regular neighbor discovery of mobile nodes. Using Fuzzy If then Rules, nodes are categorized as QoS Satisfied node or QoS unsatisfied node as shown in Fig 3.

Fig 3 QoS Forward node discovery
Figure 4 shows how shortest path is calculated using Warshalls Floyd algorithm.

Fig 4 Shortest Path Discovery
The packet is encrypted using symmetric key and it is transmitted. Using the same key, message is decrypted. Figure 5 shows both encryption and decryption process.

V. PERFORMANCE EVALUATION
To evaluate the performance of the proposed system Secure AQMRA, following performance metrics such as Packet delivery ratio, average end to end delay, Path success ratio and control overhead are evaluated for the proposed system and compared with existing AQMRA protocol.

A. Average End to End Delay
This indicates the end-to-end delay experienced by packets from source to destinations.

Fig 6 Calculating to End Delay
In Figure 6, End to End delay increases gradually when number of nodes increases. The proposed Secure AQMRA protocol is optimized for link utilization and bandwidth, so its delay is minimum when compared to existing protocol.

B. Normalised Overhead

Fig 7 Normalized overhead versus number of nodes
The System selects the QoS satisfied nodes for performing routing process. Due to secure agent
configuration of mobile nodes, unwanted routing discovery messages are eliminated and thereby it protects the system for faulty behavior. The control overhead or normalized overhead is reduced when scalability increases. This proposed scheme performs better than the existing one and its behavior is shown in Figure 7.

C. Packet Delivery Ratio

\[
PDR = \frac{\text{Number of Packets sent}}{\text{Number of Packets received}}
\]

Figure 7 Packet Delivery Ratio

The impact of PDR over number of nodes were analysed in Fig 8. When number of nodes increases <25, there exists linear increase in PDR for the proposed system. This behavior prevails as nodes are QoS enabled and designed according to user requirements and incorporated security features. From the above discussion, the proposed protocol Secure AQMRA outperforms in terms of PDR, End to End delay and Control overhead.

VI. CONCLUSION

MANET is a self established network where each node enters at any time and detach from the network. Still, ad-hoc networks are prone to millions of attacks. Attack Containment measures are used to minimize the effect of attacks. The proposed method ensures both the scalability and security of the routing protocol with privacy preservation. Neighbor discovery scheme senses multiple neighbors in its communication range. This helps to accumulate more resources from its neighbors. After discovering the secure neighbors, Optimization of QoS parameters takes place. During optimization, QoS satisfying nodes are discovered for data transmission to improve the scalability of the mobile ad-hoc network.

REFERENCES