Scientific Research Publishing

Circuits and Systems, 2016, 7, 4154-4168
http://www.scirp.org/journal/cs
ISSN Online: 2153-1293
ISSN Print: 2153-1285

Secure Multicast Tree Construction Using Bacterial Foraging Optimization (BFO) for MANET

Arthi Arumugam[1], Chinnappan Jayakumar[2]

[1]Department of Information Technology, RMK Engineering College, Anna University, Chennai, India
[2]Department of Computer Science and Engineering, Sri Venkateswara College of Engineering, Anna University, Chennai, India
Email: aarthi.punithaa@gmail.com, cjayakumar2007@gmail.com

How to cite this paper: Arumugam, A. and Jayakumar, C. (2016) Secure Multicast Tree Construction Using Bacterial Foraging Optimization (BFO) for MANET. *Circuits and Systems*, **7**, 4154-4168.
http://dx.doi.org/10.4236/cs.2016.713342

Received: April 9, 2016
Accepted: April 18, 2016
Published: November 18, 2016

Abstract

In Mobile Ad-Hoc Networks (MANET), the group communication for multiple senders and receivers threatens the security features. The multicasting is provoked to various security attacks, eavesdropping etc., hence secure multicasting requires imperative significance. The secure multicast tree construction using Bacterial Foraging Optimization (BPO) algorithm is proposed to develop a secure multicast tree construction in MANET. During routing, the proposed algorithm utilizes the public routing proxy to hide identity of the sender and receiver from other nodes for maintaining confidentiality. The public routing proxy is estimated using bacterial foraging optimization algorithm and path reliability is evaluated after the each iteration. Path reliability enhances the security of the network from black hole attacker and DoS attackers compared to traditional approaches for secure multicast tree formation in MANETs. By simulation results, we have shown that the proposed technique offers authentication and confidentiality during secure multicasting which is compared to conventional multicast tree formation algorithms in MANETs.

Keywords

Bacterial Foraging, Public Routing, Multicast Tree, *E. coli* Cell, Black Hole, DoS

1. Introduction

1.1. MANET

Mobile ad hoc network is formed by a group of many mobile nodes that are self-organized and connected with wireless links to communicate with each other without any infrastructure. Each node behaves as an end-system as well as a router to forward packets. The routing algorithm forwards a packet to the shortest path towards the source to

destination, because the mobility nature of mobile nodes is frequently changed in the network topology [1] [2] [3]. Hence, MANETs are possible types of applications such as military battlefield communication, emergency situations, emergency mitigation schemes, stock quotes, urgent business meeting, virtual class room and other [3].

1.2. Multicast Tree Construction in MANET

MANETs multicast routing protocol can be classified into two main categories: 1) topology based multicast protocol (stateful); 2) position based multicast protocol (stateless). Topology-based multicast protocols for MANETs can be considered into two main classes: tree-based and mesh-based protocols. A data dissemination tree with exactly one path from a source to each destination is formed with topological information in the tree-based approaches. The trees can be sub-classified further into source trees and shared trees. Protocols such as Multicast routing protocol based on Zone Routing (MZR) authorize each and every unique source to set up its own tree to distribute its packets if in case a shared tree empowers each and every linked node to communication packets to all remaining nodes with the help of the corresponding tree. Shared trees are built among others e.g., MAODV. Local repair mechanisms are often utilized by tree-based approaches for shielding the distribution structure from link failures due to mobility. Topology-based multicast protocols are commonly hard to scale to a substantial system size, as the construction and upkeep of the conventional tree or mesh structure involve high control overhead over a dynamic network [4].

1.3. Issues in Multicast Tree Construction in MANET

No other networks face a sensitive issue as security as in MANETs because of lack of infrastructure and the broadcast nature of the network. As MANETs have no clear line of defense, it is open to both legitimate network users and malicious attackers. When MANETs are vulnerable to many passive and active security attacks from outside by malicious nodes or from the inside by compromised nodes, effective security measures requirement is increased. Hence, designing a security solution protecting MANETs from various routing attacks with malicious nodes is a main challenge [2] [3]. The deficiency of a trusted centralized authority, easy eaves dropping due to shared wireless medium, dynamic network topology, battery power, low bandwidth and memory constraints of the mobile devices, paid the way for MANETs vulnerability to security attacks [4] [5].

The multicast state information varies with varying network topology or group membership. The frequent topology change and dynamic group membership in MANETs often result in substantial signaling overhead to maintain the global multicast session state information. If the network multicast groups are higher, this problem gets even worsen [1].

The Multicast routing in MANETs is vulnerable to various attacks like:

- Passive attacks.
- Active attacks.

- Resource consumption attack.
- Rushing attack.
- Black hole attack.
- Gray hole attack.
- Wormhole attack [5].

1.4. Secure Multicast Tree Construction in MANET

Multiple senders and receivers increase the challenge in the security issue of MANETS in group communication. Multicast security is hence more complicated than in the unicast. Many unicast solutions are prohibitively inefficient for multicast scenarios [6].

Secure ad-hoc network need the following key attributes:

1) Confidentiality to ensure payload data and header information is kept closed to unauthorized nodes.

2) Integrity to ensure that message is never corrupted.

3) Availability to ensure node services will be available to its users when required *i.e.* network services survivability despite denial of service attacks.

4) Authentication to enable a node to ensure the identity of the communicating peer mode.

5) Non-repudiation to ensure message origin cannot disclose the message transferred [3] [6] [7].

1.5. Problem Statement

Group communication for multiple senders and receivers threaten the security of MANETS. Multicasting in MANET is open to various security attacks, eavesdropping etc. Hence secure multicasting is of vital importance.

In Secure Model for Attack Detection and Authentication (SMADA) [8], the group heads are selected based on the access policy and bandwidth which is controlled by group controller elected based on the trust value. The group heads are authenticated by the controllers using shared key. The group members are authenticated based on their trust value of the node which is based on the nodes status and residual energy. When a source node wants to get connected with the destination node, its access policies and trust values are analyzed. If the trust value is below the minimum threshold and the access policy gets violated then source is denied from getting connected to the destination node.

As an extension to SMADA, SMTBFO protocol is proposed to develop a secure multicast tree construction in MANET.

The rest of this paper is organized as follows: In Section 2, some related work on MANET multicast protocols have been discussed. The proposed protocol has been discussed in section 3. In section 4, the simulation results obtained using NS-2 has been presented and the proposed protocol is compared with DIPLOMA [14] and Section 5 concludes the paper.

2. Related Works

Amandeep chhabra and Geeta Arora [3] have proposed a security mechanism for a multicast routing protocol. The Group Diffie Hellman (GDH) algorithm is utilized in this mechanism. The messages are delivered securely by using the keys which are generated by the GDH algorithm. The 1 to N nodes in the same group and the nodes in more than one group are generated with keys by this algorithm. Node communication of the Message is secure as each node use a secret key to encrypt and decrypt the message. However, it did not mention a particular routing protocol.

Mansoor Alicherry and Angelos D. Keromytis [9] have presented an architecture called DIPLOMA. It is used in multicast traffic architecture for MANET. It depends on the network capabilities. It is a deny-by-default and distributed policy enforcement architecture. It is intended to shelter the bandwidth of the network and to safeguard the end-host resources. In a multicast group, it will hinder the unauthorized sender to transfer data packets and it will hinder the unauthorized receivers to join the multicast group. To employ DIPLOMA, the popular multicast protocols like ODMRP and PIM-SM were tailored. The attackers are also quite scheduled by the DIPLOMA to protect the legitimate traffic. However, the attacker is taking up most of the bandwidth, at 8.04 Mbps.

Bhavana B. Turorikar and M. A. Shukla [10] have remodeled the existing EGMP and proposed a novel Secure Efficient Geographic Multicast Protocol (SEGMP). The efficient and scalable group membership management scheme is incorporated by SEGMP which exploits a virtual zone-based structure. In a wide environment, a zone-based bidirectional tree is created. The reason behind the creation of bidirectional tree is to attain more efficient membership management and to achieve multicast delivery of packets. The building of zone structure and multicast tree and the multicast packet forwarding uses the position information. In route searching and tree structure maintenance, this position information efficiently minimizes the route overhead. The hierarchical group membership management is employed with the zone depth to incorporate the construction of an optimal tree structure and to integrate the searching of the location of group members. Henceforth, the protocol efficiency will be increased. The zone structure empty zone problems in various routing protocols are solved by the scheme designed by them. Consequently, a scheme for the process of electing a zonal leader by voting was proposed. Thus, in the virtual zone based network, the ECDSA algorithm solves the security of votes for multicasting over MANETs. However, computational complexity exists.

Bo Rong *et al.* [11] have presented a pyramidal security model. In one co-operation domain, the multi-security level information sharing is protected by this model. This proposed security model includes three schemes namely separated star key graph, separated tree key graph and integrated tree key graph. These three schemes are used to make an efficient key management solution for the all involved multicast groups. Yet, for an individual tree key graph, the existing tree balancing approaches cannot be implemented by the sorted recursive tree known as the integrated tree key graph.

Young-Hoon Park *et al.* [12] have suggested a new GKM framework. This proposed framework works with two algorithms. The first algorithm builds a basic key-tree at the beginning to reflect the user characteristics of existing probabilities by generating an optimal key-tree. The second algorithm minimizes the communication overhead by continuing the maintenance of communication in group rekeying. However, the processing time is more.

K. Drira *et al.* [13] have proposed a framework called group key management framework. This framework depends on the trust oriented clustering scheme. The authentication is imposed by the trust information. This trust information is distributed by the feature called node mobility. In the multicast session, the malicious nodes which may be the authorized members of the group are discarded. However, this is not sufficiently stated the efficiency of the scheme.

Hyoungshick Kim and Jaehoon Jeong [14] have proposed a Recipient Anonymous Data (RAD) delivery. This technique is adopted and optimized significantly for stable-topology networks. This technique implies an efficient multicast protocol by the establishment of public routing proxy concept. The public routing proxy distributes the data to a set of "k" network entities which includes the focused receiver. Henceforth, the sender is allowed to broadcast the message to the focused receiver anonymously. This completely guarantees the proposed protocol with the receiver's k-anonymity. Yet, to guarantee and maintain the k-anonymity in each network entity's public routing proxies is more complex. This leads to increase the complexity in the mobility entity of the dynamic networks.

Mansoor Alicherry and Angelos D. Keromytis [14] have presented an architecture called DIPLOMA. It is used in multicast traffic architecture for MANET. It depends on the network capabilities. It is a deny-by-default and distributed policy enforcement architecture. It is intended to shelter the bandwidth of the network and to safeguard the end-host resources. In a multicast group, it will hinder the unauthorized sender to transfer data packets and it will hinder the unauthorized receivers to join the multicast group. To employ DIPLOMA, the popular multicast protocols like ODMRP and PIM-SM were tailored. The attackers are also quite scheduled by the DIPLOMA to protect the legitimate traffic. However, the attacker is taking up most of the bandwidth, at 8.04 Mbps.

3. Proposed Approach

3.1. Secure Route Selection Based on Bacterial Foraging Optimization Technique

Bacterial Foraging Optimization Technique is mainly based on the movement of the *E. coli* bacteria based on the nutrient content (gradient of nutrient) in the given system (area of deployment). Bacterial Foraging Optimization Technique involves the foraging of the *E. coli* bacteria in search of nutrients using the following four steps: [15]-[19]

- Chemotaxis.
- Swarming.

- Reproduction.
- Elimination and Dispersal.

Here the bacteria move from one node to another node in search of nutrients and thus forms an optimum route from the source to the destination node. Based on the nutrient content of a node and the maximum signaling between the bacteria, an optimum route is selected from among the maximum possible routes in the given network. In the given network each node's location is assumed to contain bacteria (equally distributed). Based on the nutrient content of each node and the distance between each node (or the located bacteria) is employed in calculating the signaling between the bacteria for selection of the desired route.

3.1.1. Chemotaxis

The bacteria moves in small steps in search of nutrition, by swimming or tumbling in a given direction, by sensing and communication with each other. The bacteria moves through the given (to be sensed) region, by moving with the help of flagella. Basically left-handed helical motion of flagella, *i.e.* counterclockwise motion of the attached flagella, is considered as a propulsion for the forward motion of the bacteria considered at each node.

Whereas when the direction is changed, by abruptly changing the flagella to clockwise (when rotating in the opposite direction), it moves away from the chemo-attractant direction, then the bacteria tumbles, incapable of going anywhere, hence no net displacement in the specified direction (since it moves in some new random directions).

Since each node in the network is considered to consist of bacteria, we consider node N with bacteria B. The swim and tumble (run and tumble) of the bacteria decides the direction to move in the direction of maximum nutrients by comparing the nutrient gradient in different possible paths (neighbors) that are connected to the node N.

Let us consider the nutrient gradient of the given path from the node N to node I be ∂nutrient (N,I).

3.1.2. Swarming

In this step, the self-organizing behavior of the *E. coli* bacterium is evaluated. Bacteria which reaches a more desirable location attracts a stable swarm of *E. coli* bacteria to the same location in the given network by attracting each bacteria (at each node) using signaling. Hence during tumbling, the bacteria's are drifted to a direction depending on the signaling between the bacteria from a more stable and desirable location. Hence, the total nutrient content at each node is the magnitude of the sum of signaling, between bacteria, at that given node. The signaling of bacteria at the location of I^{th} node towards the N^{th} node can be represented as follows:

$$\text{Signaling}(I,N) = \frac{A(I,N)}{e^{D_{attraction} d_{IN}^2}} - \frac{R(I,N)}{e^{D_{Repellent} d_{IN}^2}} \quad (1)$$

where,

A(I,N): Magnitude of attractant released from node I towards node N;

R(I,N): Magnitude of repellent released from node I towards node N;

d_{IN}: Distance from node I to node N;

$D_{attraction}$: Diffusion rate of attractant released from node I towards node N;

$D_{Repellent}$: Diffusion rate of repellent released from node I towards node N.

Since diffusion rate of attraction and repellent is distinct for different branches in the network, based on the amount of attractant and repellent released from each bacterium at each node in the network, they define the characteristics of the branch in which they propel. For the first iteration, a random number is considered as diffusion rate of attraction and repellent. After the first iteration, the value of diffusion rate of attraction and repellent is calculated as in Equation (2):

$$D_{attraction} = D_{Repellent} = Cost_{Network} \times \text{Diffusion Factor} \tag{2}$$

In our experiment, the value of diffusion factor employed was 0.00498 and was observed to provide with a faster convergence range. Hence after each iteration, the cost as well as the diffusion rate of attractant and repellent, released from bacteria at one node to another bacteria at another node, varies. Where the magnitude of repellent and attractants for each iteration (after the first iteration) varies as described above. Hence, the value of A(I,N) for j^{th} iteration is calculated as follows in Equation (3):

$$A(I,N) = \frac{\text{Total load in the Network generated by the movement of the bacteria in } t^{th} \text{ iteration}}{\text{Total nodes in the Network}} \tag{3}$$

Similarly R(I,N) for jth iteration is calculated as follows as in Equation (4):

$$R(I,N) = \frac{\text{Frequency of appearence of the same branch till the } j^{th} \text{ iteration}}{\text{Total number of bacteria} \times \text{Total number of nodes in the Network} \times \text{Number of Chemotatic step defined}} \tag{4}$$

Since the magnitude of repellent is dependent on the number of times a given branch occurs, hence redundant paths are reduced in the network after an initial number of iterations. For a bacteria at node N, the nutrient value at node I is Equation (5):

$$NU_I = \frac{I}{Load(I)} \tag{5}$$

In our approach since the nutrient component at a node, for a bacteria, is inversely proportional to the load at the node, bacteria during locomotion would prefer to move towards a node with least load compared to a node with a heavy load. Hence, optimum routes are preferred to travel from a source node to the destination node rather than routes with lower latency.

During tumbling, signaling between two bacteria at Ith node towards the Nth node is defined as follows in Equation (6):

$$Signaling_{Tumbling}(I,N) = NU_I / \delta_{nutrient}(N,I) + Signaling(I,N) \tag{6}$$

In our approach for fast convergence, ∂ nutrient(N,I) value is optimally set to 200.

3.1.3. Reproduction

In our proposed approach we consider the population of bacteria in a given region as

fixed. A healthy bacterium reproduces by splitting itself into two bacteria while the weak bacteria ages and dies with time. Reproduction of bacteria is helpful during the expedition of a bacterium, from the source node to the destination node, which may get trapped at local optimal Hence, reproduction helps the bacteria to explore a multiple number of nodes and path in the network. Let us consider the total number of bacteria's be BA in the overall network.

Here, BA = number of nodes in the network.

For jth bacteria, the fitness value is calculated as in Equation (7),

$$\text{Fitness} = \left(\text{Number of nodes explored by the Bacteria}\right)^{-1} \tag{7}$$

Hence, the bacteria which explore the least number of nodes have the highest fitness value compared to bacteria which has explored least nodes in the network.

3.1.4. Elimination and Dispersal

After the above-mentioned rounds, it can be observed that a bacterium visits the same branch multiple number of times. Hence, the route between node N and node I with the highest frequency of appearance is a more optimal route compares to a route with the lowest frequency of appearance.

3.2. Secured Routing

In order to hide the identity of the sender and receiver from other nodes for maintaining confidentiality, we propose a secret data delivery technique. This technique involves the distribution of secret message (P) to all the nodes which are chosen randomly and intended receiver through a public routing proxy (R). The data flow occurs as follows

Source (Data) → R → Destination

This reveals that the data from the source node is initially transmitted to R and then R transmits the data to destination. Figure 1 represents the data packet format used in our proposed method.

Here, Number of hops represents the route (number of intermediate nodes considered) during routing from source to the destination for route establishment.

The public routing proxy is estimated using bacterial foraging optimization algorithm (shown in Section 3.1) for each vertex e ∈ E, where E is the set of vertices within hop distance H(r,P) from P. The steps involved in secured routing are as follows:

1) Initially, source node S estimates the routing proxy of destination node D(Rd) and chooses randomly a routing proxy r. For r ∈ Rd around destination node D. (*i.e.* the selection of Intermediate node).

2) Source node S then transmits the message (P) to the considered random routing proxy r. Hence, this step initiates the intermediate nodes for routing the data packet

Packet Type	Source Address(As)	Destination Address(AD)	Hop(H)	Message(P)

Figure 1. Data packet format.

from the source node S to the destination node D.

3) r multicasts r to e ∈ E upon receiving the message (P) from the source node S.

This reveals that the r can forward the message P from e to vertices E by setting Time-To-Live value as hop distance H(r,P).

Consider the example shown in Figure 2.

As shown in Figure 2, the node N1 wants to deliver a message to node N5.

- Initially, N1 randomly chooses public routing proxies of N5 prior to message delivery.
- Using the algorithm, five public routing proxies are estimated.
- Also, N5 itself is included in the N5's public routing proxies.
- During this phase, we assume that N1 received the information about all network nodes' public routing proxies periodically.
- Hence, N1 delivers the message with the information about "H = 3" to the randomly chosen nodes *i.e.* R (N2 and N4) from the N5's public routing proxies.
- After receiving this message, N2 relays the messages to the nodes within 3 hops.

This routing also possesses rule that the source node can send multiple messages to the same destination node sequentially. When S wants to deliver a message to intended D, the same R need to be used repeatedly. Or else, the size of secrecy set may be minimized based on statistical inference attacks.

3.3. Path Reliability Calculation

From the route selected from source node to destination node, the path reliability is evaluated, as in Equation (8) and after the each iteration.

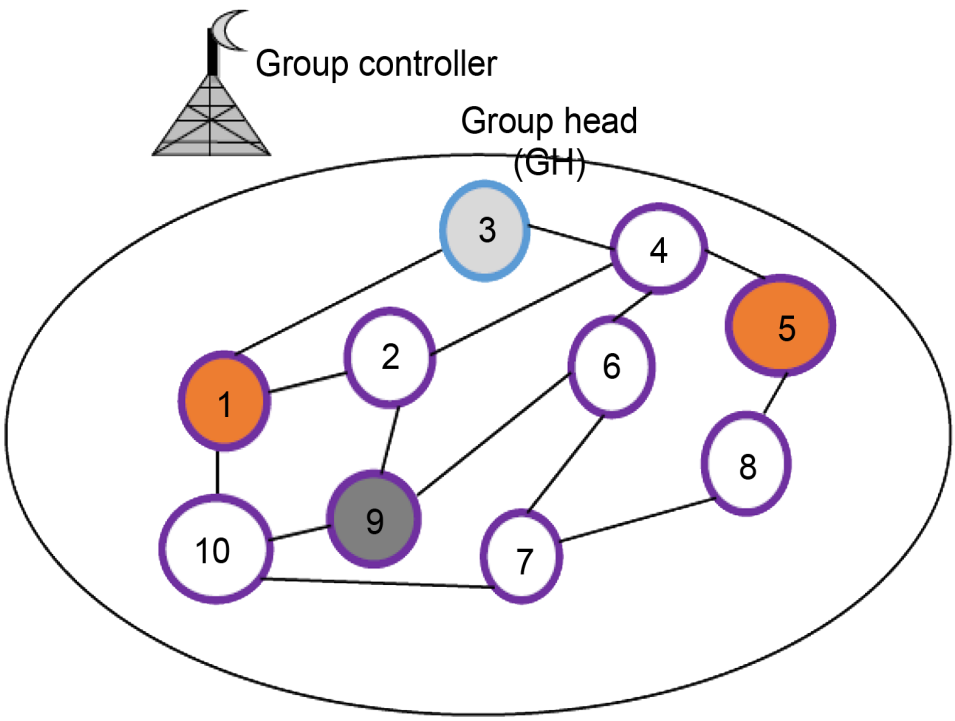
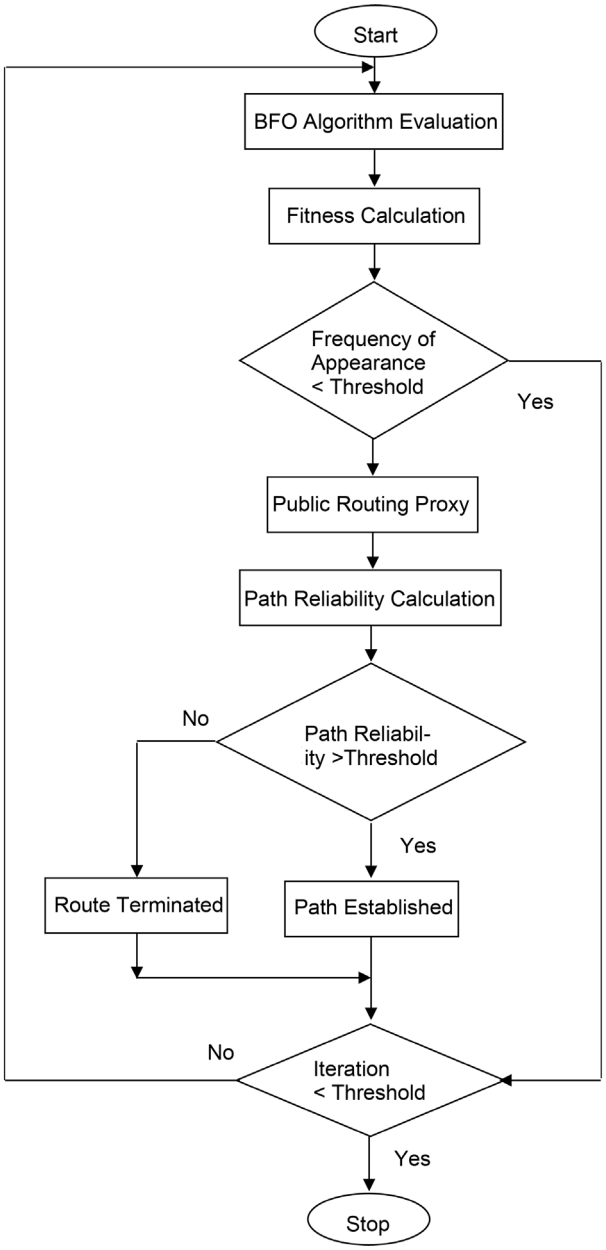


Figure 2. Route established using BFO approach.



The path with highest reliability value from node I towards node N, is the most desirable path compared to the route between the same nodes I towards node N with a different set of intermediate nodes.

$$\text{Path Reliability, PR} = \sum_{n=1}^{\text{Total number of hops}} \frac{2 - \text{fitness} - \text{packet loss rate} - \text{Number of packets sent}}{\text{Total number of packets received}} \quad (8)$$

where $0 \le PR \le 1$.

Integration of path reliability to the proposed approach helps in increasing the reliability in data communication with the least retransmission requirement. It also helps in reducing the number of attacks on the network such as black hole attack and DoS attacks.

4. Simulation Results

4.1. Simulation Parameters

Network Simulator (NS)-2 [20] is used to simulate our proposed Secure Multicast Tree construction using Bacterial Foraging Optimization protocol. In this simulation, as shown in Table 1, the mobile nodes are moving in a square region of 1000 m × 1000 m for 50 seconds simulation time. Let us assume that each node moves independently with the same average speed. All nodes have the same transmission range of 250 m. Random Way Point mobility model is used. The simulated traffic is Constant Bit Rate (CBR). This protocol uses the Distributed Coordination Function of IEEE 802.11 as the MAC layer protocol. The DCF notifies the network layer about link breakage. The channel capacity of mobile nodes is set to the value of 2 Mbps and the number of flows is 8.

The details of the simulation settings and parameters are summarized in Table 1.

4.2. Performance Metrics

We evaluate performance of the new protocol mainly according to the following parameters. We compare the DIPLOMA approach [14] with our proposed SMTBFO protocol.

Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted. The delivery ratio in a given

Table 1. Simulation parameters.

No. of Nodes	50
Area	1000 × 1000
MAC	802.11
Radio Range	250 m
Simulation Time	50 sec
Traffic Source	CBR
Rate	250 Kb
Packet Size	512 B
Mobility Model	Random Way Point
Routing Protocol	SMTBFO
Pause Time	5 Seconds
Rx Power	0.395
Tx Power	0.660
Idle Power	0.035
Initial Energy	12.1 J
No. of Receivers	5
No. of Attackers	1, 2, 3, 4 & 5

network should be high compared to a weak network.

Resilience: It is the ratio of fraction of data packets affected to the number of malicious activities during the data transmission.

Energy: It is the amount of energy consumed by the nodes for the data transmission.

The simulation results are presented in the next section.

4.3. Results & Analysis

Effect of varying Attackers

In the experiment results are varying the number of attackers as 1, 2, 3, 4 and 5.

4.3.1. Attackers vs. Delivery Ratio

From Figure 3, it can be seen that the effectiveness of SMTBFO is high compared to the existing DIPLOMA approach. The packet delivery ratio of the proposed SMTBFO is 22% higher than the existing DIPLOMA protocol. Even if the number of attacker nodes is increased from 1 to 5, still the delivery ratio of the network is efficient in comparison with the existing traditional approaches. Dropping of data packets also leads to minimal delivery ratio in a network. Hence, an outside/inside attacker hampers the overall performance of the network. By using SMTBFO even under such a scenario the network can be made reliable and efficient.

4.3.2. Attackers vs. Energy Consumption

For an efficient network, to enhance the network lifetime and usefulness, the energy consumption (dissipation) at each node in the network should be minimal. From Figure 4, it can be seen that the consumption energy of the proposed SMTBFO is 5.3% less than the existing DIPLOMA protocol. Hence using SMTBFO the energy consumption

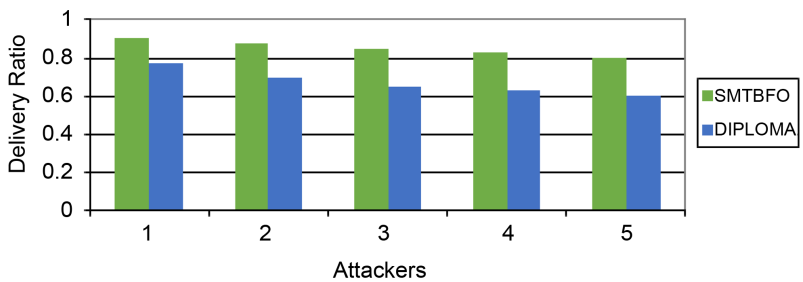


Figure 3. Attackers vs. delivery ratio.

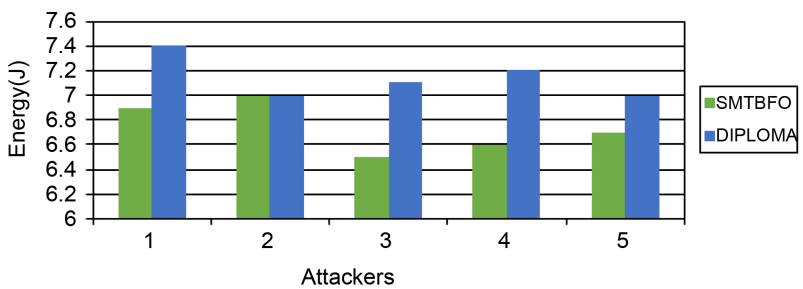


Figure 4. Attackers vs. energy consumption.

in the network is minimized even in the presence of multiple attacker nodes. When the number of attacker nodes are increased from 3 to 5, energy consumption in the whole networks falls down to a minimal value. Hence even in the presence of multiple nodes (even more than 5 attacker nodes) the proposed approach is very efficient compared to previous approaches.

4.3.3. Attackers vs. Resilience

Attacker nodes are capable of altering the data packets and also dropping data packets. Such attackers reduce the reliability of the network and eventually mislead the communication and destroy the truthfulness (purpose) of the network. Resilience is the ratio of fraction of data packets affected to the number of malicious activities during the data transmission. From Figure 5, it can be seen that the resilience of the proposed SMTBFO is 24.1% less than the existing DIPLOMA protocol. SMTBFO hence provides high immunity towards attackers which in turn reduces the number of data packets affected during data transmission.

4.3.4. Attackers vs. Drop

For an efficient network the drop at each node should be minimal even in the presence of attacker nodes. From Figure 6, it can be seen that the packet drop of the proposed SMTBFO is 70.1% less than the existing DIPLOMA protocol.

5. Conclusion

In this paper, we have proposed algorithm to develop a secure multicast tree construction in MANETs. Since black hole attack leads to dropping of packets without its delivery to the destination, it keeps the sender waiting for an acknowledgement till it dies

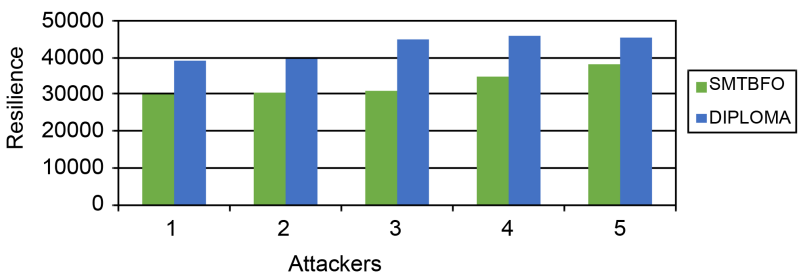


Figure 5. Attackers vs. resilience.

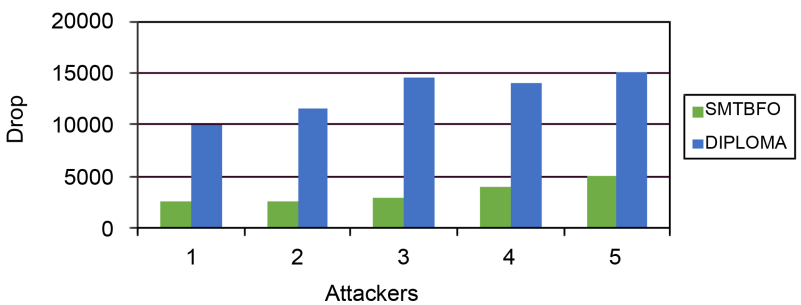


Figure 6. Attackers vs. drop.

of inefficient energy. Similarly, DoS attack floods the network with unwanted data packets, hence reducing the residual energy of the overall network leading to reduction in the usefulness of the network. Our proposed algorithm is found to be highly reliable and robust against such attacks leading to increase in the usefulness and trustworthiness of the network.

References

[1] Chen, K. and Nahrstedt, K. (2002) Effective Location-Guided Tree Construction Algorithms for Small Group Multicast in MANET. *IEEE INFOCOM*, New York, June 2002, 1180-1189.

[2] Olagbegil, B.S. and Meghanathan, N. (2010) A Review of the Energy Efficient and Secure Multicast Routing Protocols for Mobile Ad Hoc Networks. *International Journal on Applications of Graph Theory in Wireless Ad Hoc Networks and Sensor Networks*, **2**, 232-250. http://dx.doi.org/10.5121/jgraphoc.2010.2201

[3] Chhabra, A. and Arora, G. (2013) Secure Routing in Multicast Routing Protocol for Manet's. *International Journal of Innovations in Engineering and Technology*, **2**, 1-8.

[4] Karbhal, J.M. and Sadafale, K.B. (2013) Secure Efficient Geographic Multicast Protocol for Mobile Ad Hoc Networks. *International Journal of P2P Network Trends and Technology*, **3**, 62-66.

[5] Vijayalakshmi, S. and Albert Rabara, S. (2011) Weeding Wormhole Attack in MANET Multicast Routing Using Two Novel Techniques-LP3 and NAWA2. *International Journal of Computer Applications*, **16**, 26-32. http://dx.doi.org/10.5120/2024-2729

[6] Rajan, C. and Shanthi, N. (2013) Misbehaving Attack Mitigation Technique for Multicast Security in Mobile Ad Hoc Networks (Manet). *Journal of Theoretical and Applied Information Technology*, **48**, 1349-1357.

[7] Gomathi, K. and Parvathavarthini, B. (2010) An Efficient Cluster based Key Management Scheme for MANET with Authentication. *Trends in Information Sciences & Computing*, **10**, 202-205. http://dx.doi.org/10.1109/TISC.2010.5714639

[8] Arthi, A., Jayakumar, C. and Tanguturi, R.C. (2014) SMADA—Secure Model for Attack Detection and Authentication of Multicast Routing in MANET. *International Journal of Applied Engineering Research*, **9**, 9438-9446.

[9] Alicherry, M. and Keromytis, A.D. (2010) Securing MANET Multicast Using Diploma. *Advances in Information and Computer Security*, **10**, 232-250. http://dx.doi.org/10.1007/978-3-642-16825-3_16

[10] Turorikar, B.B. and Shukla, M.A. (2013) Multicasting over Manet through Segmp by Secure Zone Leader Election. *International Journal of Computer Trends and Technology*, **4**, 153-159.

[11] Rong, B., Chen, H.-H., Qian, Y., Lu, K.J., Hu, Q.Y. and Guizani, S. (2009) A Pyramidal Security Model for Large-Scale Group-Oriented Computing in Mobile Ad Hoc Networks: The Key Management Study. *IEEE Transactions on Vehicular Technology*, **58**, 398-408. http://dx.doi.org/10.1109/TVT.2008.923666

[12] Park, Y.-H., Je, D.-H., Park, M.-H. and Seo, S.-W. (2013) Efficient Rekeying Framework for Secure Multicast with Diverse-Subscription-Period Mobile User. *IEEE Transactions on Mobile Computing*, **99**, 1-14.

[13] Drira, K., Seba, H. and Kheddouci, H. (2010) ECGK: An Efficient Clustering Scheme for Group Key Management. *Computer Communications*, **33**, 1094-1107.

http://dx.doi.org/10.1016/j.comcom.2010.02.007

[14] Kim, H. and Jeong, J. (2011) RAD: Recipient-Anonymous Data Delivery Based on Public Routing Proxies. *Computer Networks*, **55**, 3469-3484. http://dx.doi.org/10.1016/j.comnet.2011.07.009

[15] Bitam, S., Mellouk, A. and Zeadally, S. (2015) Bio-Inspired Routing Algorithms Survey for Vehicular Ad Hoc Networks. *IEEE Communication Surveys & Tutorials*, **17**, 843-867.

[16] Sodsri, P., Sookananta, B. and Pusayatanont, M. (2015) Optimal Placement of Distributed Generation Using Bacterial Foraging Optimization Algorithm. *AMM*, **781**, 329-332. http://dx.doi.org/10.4028/www.scientific.net/AMM.781.329

[17] Singh, S., Ghose, T. and Goswami, S. (2012) Optimal Feeder Routing Based on the Bacterial Foraging Technique. *IEEE Transactions on Power Delivery*, **27**, 70-78. http://dx.doi.org/10.1109/TPWRD.2011.2166567

[18] Kaur, R. and Kaur, B. (2014) Artificial Neural Network Learning Enhancement Using Bacterial Foraging Optimization Algorithm. *International Journal of Computer Applications*, **102**, 27-33.

[19] Schweitzer, N., Stulman, A., Shabtai, A. and Margalit, R. (2016) Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes. *IEEE Transactions on Mobile Computing*, **15**, 163-172. http://dx.doi.org/10.1109/TMC.2015.2409877

[20] Network simulator. www.isi.edu/nsnam/ns