IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 10, October 2021

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010064 |

Reducing Routing Misbehavior in Dynamic Source Routing Protocol using Modified Distributed Trust Model and FG Model for Wireless Adhoc Networks

Rajani K C, Dr. Aishwarya P

Assistant Professor, Dept. of ISE, Sri Krishna Institute of Technology, Bangalore, India

HOD, Dept. of CSE, Atria Institute of Technology, Bangalore, India

ABSTRACT: Routing is an important role in modern communication networks. In WANs malicious nodes are the abnormal nodes which lead to security and routing problems. The paper represents a distributed trust model to identify malicious nodes in WANETs. The mechanism depends on the distributed trust model on each node, which is based on the reputation value computed for that kind of node by its neighboring node. The reputation information is collected, archived and interchanged between the nodes. We distinguish the performance of the proposed scheme in terms of two metrics throughput and traffic overhead under malicious attacks. By comparison of proposed model with normal distributed trust model proposed model performs better in all two categories. To minimize total control traffic overhead we have included Friendly Group model with distributed trust model so that it reduces the traffic overhead.

KEYWORDS: Wireless Ad-Hoc Networks (WANs), FGA (Friendly Group Architecture)

I. INTRODUCTION

Wireless ad hoc networks (WANs) is a rambling collection of mobile nodes that forms a network without using any pre-existing network infrastructure such as access points or base stations. A routing protocol is used to establishthe routes between nodes and flow of data from sender to receiver node. Now a days it is observed that important routing protocols[1][2][3][4] in WANs. In WANs because of less transmission range of wireless network interfaces each node acts or operates as both router and host. Thus data packets from source node transmitted over a set of intermediate nodes to receiver node. All the nodes in WANs are required to communicate packets on-behalf of other nodes however a node may behave abnormal by agreeing to send packets and fails to do so, because it is overloaded selfish or malicious. A selfish node is a node which is not willing to spend battery life or bandwidth to forward packets to other nodes. A malicious node which is abnormal node which doesnot send the packets in correct routing path it redirects packets in another routing path and leads to denial-of-serviceattacks, these abnormal nodes highly degrade the network performance. Misbehaving nodes have security problem in WANs.

However, current important ad-hoc networks routing algorithms are DSR (Dynamic source Routing) [4], AODV (Ad Hoc On Demand Distance Vector) [3]and DSDV (Destination Sequenced Distance Vector) [2]. In order to motivate nodes to behave as normal nodes, a distributed trust model [1] is used to give nodes stimulus to achieve work. In addition, because of the absence of commonly trusted nodes in WANs, the reputation system is adopted in each and every node. However, a node may give conflicting recommendations as a result of distributed reputation systems must be robust against both untruthful and inconsistent recommendations. To address these problems mentioned above, trust based intermediate nodes selection mechanism is proposed to motivate nodes to co-operate with each other to reduce malicious nodes that becomes as routing nodes. Based on DSR the proposed distributed trustbased mechanism helps to find reliable routing path. In this paper both misbehavior problem and distributed trust reputation system in ad-hoc networks are briefly discussed. Instead of proactive method, this paper adopts on-demand to acquire information from adjacent neighbors. In this way significantly communication overheads are reduced. The advantage of this information provided proposed system will be measured and the metrics of proposed system is analyzed through throughput and

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010064 |

traffic overhead. The trust model is deployed with Friendly Group model where this model helps to reduce traffic overheads. The relevant cost of obtaining recommendation using different reputation algorithms is differentiated. The proposed routing algorithm is reliable in constantly changing networks. By performance wise both analytical and simulation results we notice that proposed scheme distributed trust-based reputation system with FG model performs better than existing distributed trust model. The remainder of this paper is categorized as follows: In section II, Existing works are discussed, The proposed methodology is detailed in section III.In section IV, simulation results and performance analysis are given. In the last section, we discuss the conclusions of our research work.

II. RELATED WORKS

In this section, we briefly describe the concepts of reputation systems. There are 2 types of reputation systems centralized and distributed frameworks .Example Amazon is a centralized reputation system. With a single trust authority controls all reputation information: such systems are inflexible.Therefore centralized systems are not applicable to peer-to-peer networks.Alfarez [5] first proposed a distributed recommendation trust evaluation model for internet communication. In recent years several trust and reputation models have been introduced to improve security and significant routing in ad-hoc networks [6][7][8].A reputation system is a mechanism which is used to construct trust in ad-hoc networks and to analyze, evaluate node's behavior. Any node can judge the trustworthiness of the nodes in which they are interested. The node with highest trust value will be selected as a route node in ad-hoc networks when there are more choices, possibly abnormal nodes such as malicious and selfish nodes would not be selected as routing nodes. In addition important schemes are used to motivate nodes co-operation in the system while punishment schemes are used to punish malicious nodes.

Reputation systems monitor node's behavior by collecting, aggregating and distributing results as recommendations to the requested node. Any node gathers such collection from its own experience and secondhand data gathered from raters. A rater provides ratingdata about the rate's behavior to the requestor. The main task of reputation system is to find the truthfulness of such recommendations. The reputation system should not only keep track of transactional behavior but it also should also consider unhonestful recommendations such unhonestful recommendations overstate trustworthiness of a node.

There are two types of aggregating methods for reputation systems: global and local reputation ratings within a global reputation system, there is only one single reputation value does not depend on which node requesting it.Local reputation systems however, provide different reputation values between different groups of nodes. They provide a computation of reputation to each node. Global reputation systems were found to be wide spread collusion, they support more accurate and fast ways to detect misbehavior nodes opposite to local reputation systems. Some reputation systems are discussed as follows:

A. CORE

CORE, a collaborative reputation mechanism proposed by Michardi and Molva [8], supports three types of information: subjective, second-hand, and functional reputations. An information table is used to store sets of reputation information and a watchdog mechanism is used for detecting its neighbors' nodes behaviors. The drawback of this mechanism is that nodes only exchange positive reputation information, thus false praise makes malicious nodes harder to detect.

B. CONFIDANT

CONFIDANT, a cooperation of nodes – fairness in dynamic ad-hoc networks proposed by Buchegger and Boudec [9], provides a method to detect and isolate misbehavior nodes. In this mechanism, each node has four components: Monitor, reputation system, trust manager, and path manager. In CONFIDANT mechanism, each node only exchanges negative information. It suffers from false accusation. To overcome such problems, authors [9] presented a new reputation evaluation approach based on Bayesian learning technique [11]. In thisapproach, the first-hand information is exchanged frequently and the second-hand information is merged, if it is compatible with current reputation rating.

C. OCEAN

Bansal and Baker proposed an Observation-based Cooperation Enforcement in Ad Hoc Networks (OCEAN) [10].

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010064 |

In contrast to CORE and CONFIDANT, OCEAN avoids second-hand reputation information and uses only first-hand observations of its neighbor nodes' behavior. OCEAN has five components in each node to direct and mitigate misbehavior: Neighbor Watch, Route Ranker, Rank-Based Routing, Malicious Traffic Routing, and Second Chance Mechanism. OCEAN focuses on how to maintain the overall packet throughput of WANs having the existence of misbehaving nodes at the routing layer.

D. LARS

Hu [5] proposed a scheme called Locally Aware Reputation System (LARS). Different from global reputation schemes, such as CONFIDANT and CORE, this mechanism uses local reputation only. Each node only keeps the reputation values of all its one-hop neighbors. When an uncooperative node is detected, its k-hop neighbors become aware of the misbehavior. To avoid false accusation, conviction of the uncooperative node is co-signed by *m* different nodes. LARS uses the threshold cryptography scheme to sign the warning message about a misbehaved node.

III. TRUST BASED REPUTATION FRAMEWORK

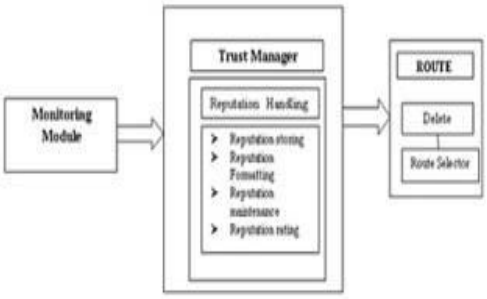

Fig 1: Architecture of Modified Trust Model

In this section, distributed based trust reputation mechanism is proposed. The proposed mechanism improves the security of routing protocol by this model and DSR routing protocol. It helps DSR to find a reliable routing path with less malicious nodes .The goal of proposed framework is to make reputed system against malicious problem, control traffic overhead and improve the efficiency of detecting malicious nodes. Figure 1 illustrates frame work of proposed system .It consists of three components Monitor, Trust Manager and Route selector.

A. Notations

A,B,C: Nodes with in network

r(A,B): node A computes reputation of node B

φ: reputation value that can take value between 0 and 1

r_{reptab}(A,B): previously stored reputation value of B

$r_{current}$(A,B): new reputation value of node B

N1…….Nn-1: WANET has n number of nodes

B. MONITORING MODULE

Each node in the network independently monitors the packet forwarding activities of its neighbors. The monitoring of node is related to the proportion of correctly forwarded packets with respect to the total number of packets forwarded in a time interval. Based on statistics if a node is misbehaved it informs to trust manager

C. REPUTATION HANDLING MODULE

The main functionality of the trust manager is reputation information management. This functionality involves four activities.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010064 |

(i) Reputation information collection
(ii) Reputation information formatting
(iii) Reputation information maintenance
(iv) Reputation information rating.

Reputation information collection:Reputation information is collected in two ways, Sensing or direct monitoring and recommendations .Each and every node within the network sends reputation request asking for its recommendations.Example: Assume that, two nodes A & B are in WANET and the node A detects that B is dropping packets. However A will not broadcast this information to its neighbors unless B's packets dropping rate crosses a predefined threshold value.

Reputation information formatting: The neighboring nodes in the WANET must exchange the reputation information among each other.In order to exchange information it uses REP_MESS messages.REP_MESS consists of three fields.REP_MESS_TYPE, NODE_ID, REP_VALREP_MESS_TYPE are of three categories.REP_REQUEST, REP_RESPONSE, REP_BROADCAST

The REP_REQUEST message is used to request for recommendations from its neighbors about a new node that is willing to join the network. ROR-Response message used by a node for replying to a recommendation request.

ROP-Broadcast message type is used when a node needs to broadcast some reputation information.

NODE_ID: IP address of the malicious node or new node that is willing to join the network.

ROP_VAL: Reputation value of the node with misbehavior has computed and stored in reputation table.

Reputation information maintenance

The reputation information is evaluated at each node before it is stored or broadcasted. Reputation table is used for storing reputation information for each of its neighbors.

Reputation rating: Reputation value for a node is a number that can take values between 0 and 1.At the beginning phase of the system, every node as reputation value 1.Reputation value for a node decreases if it exhibits any misbehavior. Node A computes reputation of node B.

$$r(A,B) = \frac{\text{Number of packets forwarded}}{\text{Total number of packets sent}} \quad (1)$$

If node A detects misbehavior of node B it needs to combine the new reputation value of node B with its previously stored reputation value .The factor φcan take a value between 0 and 1.The value r(A,B) is sum of two components.

$$r(A,B)=(1-\varphi)* r_{reptab}(A,B)+\varphi*r_{cuurenttab}(A,B) \quad (2)$$

Let us assume WANET has n number of nodes denoted as : $A,N_1, N_2,-------,N_{n-1}$ .Suppose new node D wants to join the network ,the node A detects the presence of node D and broadcasts a reputation request for node D in its neighbor node.If the node A receives response from P number of neighbors then Node A computes reputation value of node D using (u) as follows.

$$r(A,D)=\frac{\varphi*r_{reptab}(A,B) + \sum_{i=1}^{p}\left(r_{reptab}(A,Ni)*r_{reptab}(Ni,D)\right)}{\varphi+\sum_{i=1}^{p}(r_{reptab}(A,Ni))\varphi \ \sum_{i=1}^{p}(r_{reptab}(A,Ni))}$$

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010064 |

D. ROUTE SELECTOR

According to the reputation value, from the reputation managing component chooses good routing path to transfer data. If malicious nodes are found in the routing path, that path would not be selected as a routing path.

REDUCING OF TOTAL CONTROL TRAFFIC OVERHEAD BY DIVIDING A WANET INTO FRIENDLY GROUPS

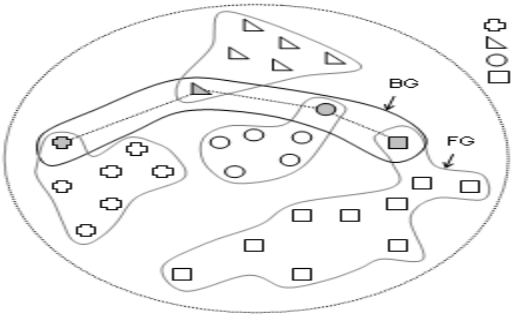

Figure 2: Friendly Group Architecture of four FG with one BG

We can minimize the total control traffic overhead by dividing a MANET into several friendly groups suitable for some applications. In FG Model [12] a network is divided using severalfriendly groups using two NICs installed in each node. The proposed diagram in Figure 3 shows the proposed Friendly Group structure. In which the four different FGs are indicated by cross,triangle, circle and square. Where, FG denotes Friendly Group and BG denote Border Group as defined in [12].The advantage of the inclusion of FG model with our model is that it minimizes the battery usage and thus enhances the network cooperation. The nodes have fewer chances for misbehaving because they have enough energy to survive. The FG Model gives a reduction in control packets as it divides a MANET of size N into k friendly groups with an approx N/k number of nodes per group. The total control overhead defined for reactive routing protocols [12] is N2 with a flat structure and in FG (Hierarchical) structure it is N2/k. This will enhance the network throughputof our proposed model up to a ratio of [k : 1 | k > 1]. The simulation result shows the benefits ofReduction in overhead after inclusion of FG model with our model.

IV. SIMULATION RESULTS AND PERFORMANCE ANALYSIS

TABLE I. Simulation parameters and their values

Parameter	Value	Parameter	Value
trSimulation Time	900(s)	Pause Time	30(s)
Simulation Area	1000 m × 1000 m	Traffic Type	CBR(UDP)
Number of Nodes	50	Maximum Connection	30
Transmission Range	250 m	Payload Size	64 bytes
Movement Model	random waypoint	Send Interval	0.5
Maximum Speed	10 m/s		

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010064 |

This paper discusses the comparison between normal distributed trust model and the proposed system simulation focus on throughput, Reputation overhead under malicious attacks and also traffic control overhead.

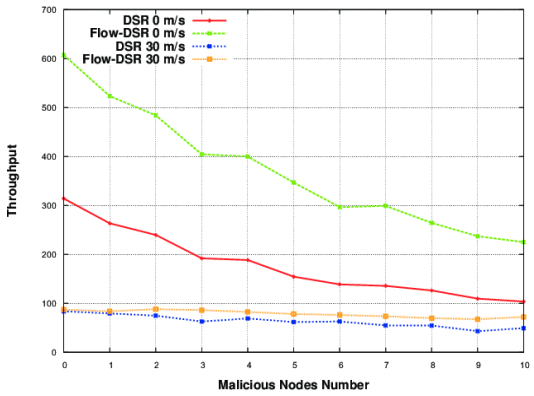

Fig 1: Good Throughput Under Malicious Attack

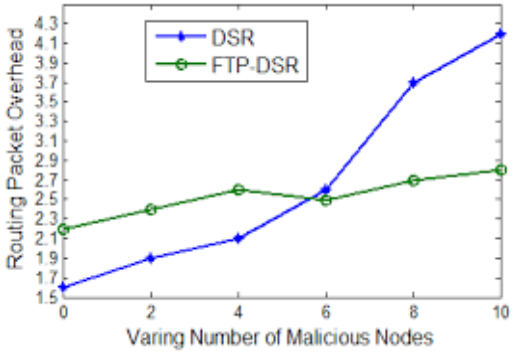

Fig 2: Reputation Byte Overhead Under Malicious Attack

V. CONCLUSIONS

In this Paper, we propose a distributedbased trust

reputation mechanism with FG model for DSR routing protocol in ad-hoc networks. The proposed mechanism is used to reduce the routing misbehavior problem. Monitoring, reputation handling and route selector are used to support this methodology. The Friendly group Model is used to reduce traffic overhead. Distributed Trust model computes the reputation of each node. The proposed paper provides atrust model to identify malicious nodes and avoids these nodes becoming as routing nodes.We compared the performance of the proposed scheme with distributed trust model and modified trust model by two metrics throughput and traffic overhead under malicious attacks.By comparison we observe that proposed mechanismperforms better than normal trust modelin two categories .The simulation results indicate that proposed mechanism stimulate nodes to co-operate with each other and improve performance of WANs.

REFERENCES

[1] A.R. Alfarez and H. Stephen, "A Distributed Trust Model," *Proceeding of 1997 New Security Paradigms Workshop, ACM press*, Cunbria, UK, pp. 48-60.

[2] C.E. Perkins and E.M. Royer, "Ad-Hoc On-Demand Distance Vector Routing," *Proceedinga of 2nd IEEE Workshop on Mobile Computing Systems and Applications*, Feb., 1999.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 10, October 2021 ||

| DOI:10.15680/IJIRSET.2021.1010064 |

[3] D.B. Johnson and D.A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," *Mobile Computing, Kluwer Acdemic Publishers*, Vol.353, 1996, pp. 153-181.
[4] Z.J. Haas, "A New Routing Protocol for the Reconfigurable Wireless Networks," *In Proceeding of the IEEE International Conference on Universal Personal Communications*, 1997
[5] L. Buttyan and J.- P. Hubaux, "Nuglets: a virtual Currency to Stimulate Cooperation in Self Organized Mobile Ad Hoc Networks," Technical report No. DSC/2001.
[6] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad Hoc Networks," *In Communications and Multimedia Security,* 2002, pp. 107-121.
[7] S. Bansal and M. Baker, "Observation-based Cooperation Enforcement in Ad Hoc Networks," *Technical Report*, 2003.
[8] S. Buchegger and J.-Y. L. Boudec, "The Effect of Rumor Spreading in Reputation Systems for Mobile Ad Hoc Networks," *In WiOpt'03: Modeling and Optimization in Mobile*, Ad Hoc and Wireless Networks,March, 2003.
[9] J. Hu, "Cooperation in Mobile Ad Hoc Networks," *Technical Report*,Computer Science Department, Florida State University, January 11, 2005.
[10] Z.J. Haas, "A New Routing Protocol for the Reconfigurable WirelessNetworks," *In Proceeding of the IEEE International Conference onUniversal Personal Communications*, 1997.
[11] Shi-Hong Chou,chi-chun Lo chuncheihHuang,*"Mitigating Routing Misbehavior in DSR protocol usingTrustbasedMechanism for ad hocnetworks"* IEEE consumer communications and Networking conference,2011.
[12] Sahoo and Akthar*"Friendly group architecture for MANETS"*International conference 2011.
[13]A Review on Multicast

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details