ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

A Trust Based Routing Protocol with Key Management

Ambily Mohan, Vidhya P M

Final Year M.Tech, Dept. of Computer Science & Engineering, Sree Narayana Gurukulam College of Engineering, Kerala, India

Assistant Professor, Dept. of Computer Science & Engineering, Sree Narayana Gurukulam College of Engineering, Kerala, India

ABSTRACT: Mobile Ad Hoc Network (MANET) consists of set of independent mobile nodes communicate via radio waves. The nodes in the MANET are constantly moving and have no fixed topology. Due to these features the intermediate nodes take part in communication must trust each other. The proposed system calculates the global trust value of each node in the network using direct and indirect method. The malicious nodes in the network can be identified and eliminated. The communication between the nodes must take place only through the most trusted path in the network. It then monitor single node failure in the trusted path during data communication and finds most trusted next node of the failed node in the route through an alternate path. When a new node enters into the network the key server verifies the validity of the requesting node by checking for its trust value with the neighbors. If it is valid then authenticate it by the key server otherwise discard it from the network.

KEYWORDS: Direct Trust, Indirect Trust, MANET, PDR

I. INTRODUCTION

MANET is a collection of independent mobile nodes and its topology changes dynamically. When a source communicates with the destination, intermediate nodes route the packets. So the intermediate nodes must trust each other.

Trust

Trust can be defined as the degree of belief that nodes in the network correctly perform the task. The five basic properties of trust in MANET are subjectivity, dynamicity, nontransitivity, asymmetry and context dependence [1].

- **Subjectivity:** The observer node in the network has a right to find out the trust value of an observed node.
- **Dynamicity:** Based on the behavior of each node, its trust value varies dynamically.
- **Nontransitivity:** If node X trust node Y and node Y trust node Z then node X doesn't trust node Z.
- **Asymmetry:** If node X trust node Y then node Y doesn't trust node X.
- **Context dependence:** Trust value of a node dependent on its behavior in the network.

The paper is organized as follows. Section I focus on Trust in MANET. Section II contains the background works related to the proposed system. Section III is devoted to detailed explanation of Proposed System. Section IV shows the simulation results. Conclusion and future work of the paper is included in section V.

II. RELATED WORK

Zhexiong Wei et al. [1] proposed a unified trust management scheme to improve the MANET security. The global trust value of each node in the network is the combination of trust value from direct and indirect observation. The direct trust is calculated using Bayesian inference and Dempster-Shafer theory is used for the calculation of the indirect trust. The node with low trust value is eliminated by the routing algorithm and establishes more secure routing path in malicious environment.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Pallavi Khatri et al. [2] introduced a composite identity and trust based model which is a modified DSR routing protocol. The node in the network is authenticated using trust factor along with the key pair and identity of a node. After the authentication, a valid certificate is issued for authentic node to take part in communication.

G.Rajkumar et al. [3] designed a short alternate path protocol. This protocol identifies link breaks or path failure during data communication and finds most trusted next node of the failed node in the route through an alternate path. This saves energy and catches the dropped packets at path failure.

III. PROPOSED SYSTEM

MANET has become the most commonly used communication technology in military environments. Trusting each node in the network increases the MANET security.

A. Block Diagram of Trust Based System

Figure 1: shows the block diagram of trust based system. The Trust module consists of Trust storage, Find and Update Trust, Direct Trust, Indirect Trust. Trust module calculates the trust value of each node using Direct and Indirect Trust value. The calculated trust value is stored in the Trust storage area. The Networking module establishes most secure trusted path between source and destination node. The Application module actually transfers data through the trusted path during communication.

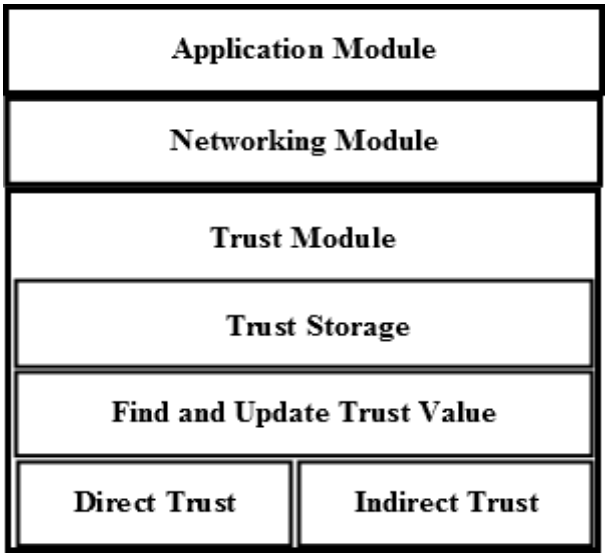

Figure 1: Block Diagram of Trust Based System

B. Alternate Node Path Discovery

During the data transmission each node in the trusted path checks whether the next node in the path are capable of receiving and transmitting the packets. If a node successfully receiving and transferring the packet to the next node then transmission continues. If a node become weak or fail finds most trusted next node of the failed node in the route through an alternate path.

Let S and D be the source and destination node respectively. During communication S sends packets to D. Each node buffers the packets before send to the next node. If there a node failure occurs at node 2 then node 1 finds most trusted next node of the failed nod public e in the route through an alternate path and transfer the buffered packets to the next node 5.

The network showed in figure 2: indicates the node failure occurs during the trusted path communication between source and destination node. Figure 3: shows the alternate node path discovery when node failure occurs in trusted path.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

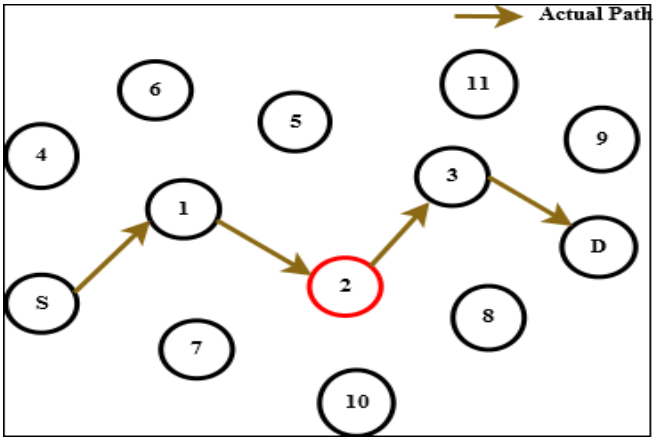

Figure 2: Node failure occurs during communication

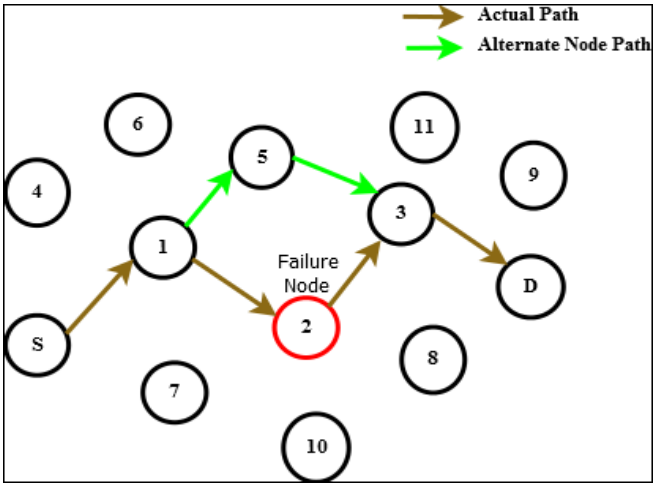

Figure 3: Alternate Node Path Discovery

C. New Node Authentication

To achieve next level of security, each node in the network has a Public key, Node ID, trust value [3]. The public key is generated and issued by Key server. When a new node trying to join in the network. It acquires public key from nearest neighbor. Then the public key, Node ID is sending to the Key Server through a trusted path. The Key Server verifies the validity of the requesting node. If it valid then added to the network, otherwise discard it. The Figure 4: shows the authentication of a new node.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

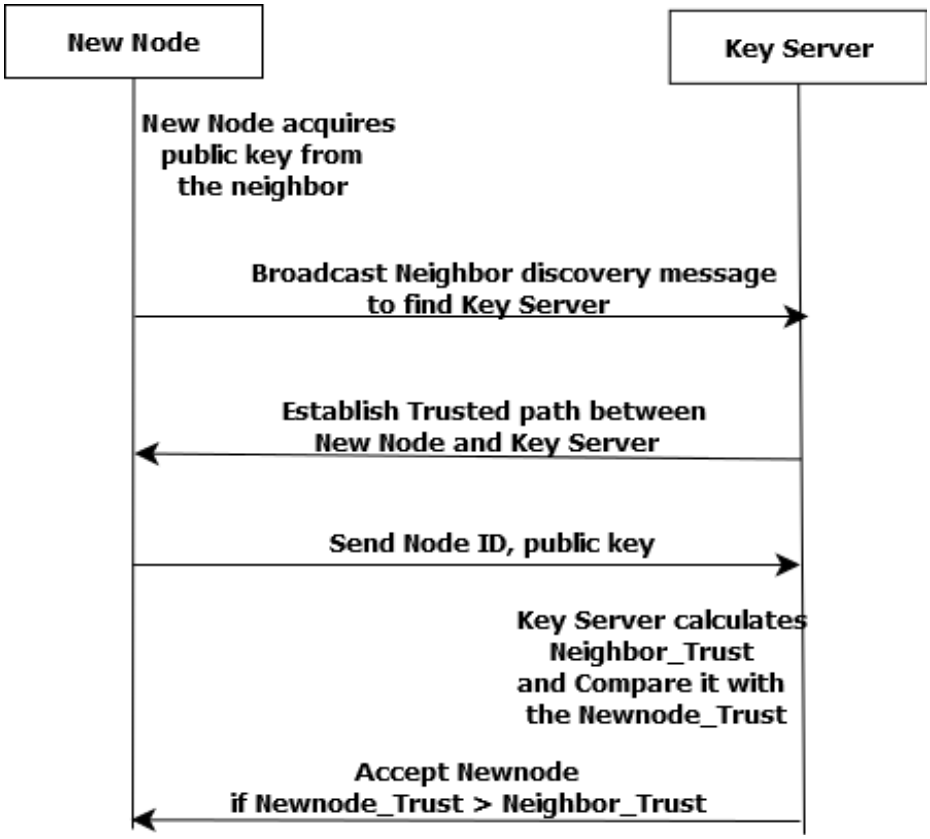

Figure 4: New Node Authentication

D. Proposed Algorithm

1. For every node in the network
   - 1.1. Calculates PDR (Packet Delivery Ratio), mobility, previous trust value, number of neighbors to the node.
   - 1.2. PDR = Number of packets received/ Number of packets forwarded.
   - 1.3. If PDR > 1 then set PDR = 1.
   - 1.4. Direct_trust = PDR.
   - 1.5. Indirect_trust = mobility value + previous trust value + number of neighbors
   - 1.6. Global_trust = Direct_trust + Indirect_trust
2. Assign high trust value node as Key Server.
3. Key Server generates the public key and broadcast it to all nodes in the network.
4. Find the most trusted path between Source and Destination node.
5. Periodically monitor single node failure in the trusted path.
6. If node failure occurs find the alternate path.
7. When new node enters into the network.
   - 7.1. New node acquires public key from the neighbor node.
   - 7.2. Broadcast NODE_DISCOVERY message into the network to identify the Key server.
   - 7.3. New node sends its Node ID, Public key to the key server.
   - 7.4. Key server verifies the requesting node.
     - 7.4.1. Find the Newnode_Trust value.
     - 7.4.2. Calculate Neighbor_Trust value.
       - 7.4.2.1. Neighbor_Trust=Some of the trust value of new node neighbors.
     - 7.4.3. If Newnode_Trust > Neighbor_Trust
       - 7.4.3.1. Accept new node and it is added to the network.
     - 7.4.4. Else

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

7.4.4.1. Discard new node and it is removed from the network.

IV. SIMULATION RESULTS

Network simulator 2.35 is used as the simulation tool for the evaluation of proposed system. The Table 1: show the simulation parameters and its value used in the NS 2.35 for the simulation of the proposed network.

A. Simulation Parameters

Parameter	Value
Application_Protocol	CBR
Transport_Protocol	UDP
Routing_Protocol	DSR
MAC_Protocol	IEEE 802.11
Queue_Type	CMUPriQueue
Propagation_ Model	Two-ray ground
Channel_Type	Wireless Channel
Antenna_Type	Omni directional
Number of Nodes	50
Simulation_Area	900m x 600m

Table 1: Simulation Parameters

Initially all the nodes in the MANET are randomly placed in the defined area. Each scenario has a pair of source and destination nodes. The node with the high trust value is set as Key server.

Figure 5: shows the source to destination communication in MANET. Communication takes only through the most trusted path between source and destination node. Figure 6: indicates alternate node path selection when node failure occurs in the trusted communication path.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

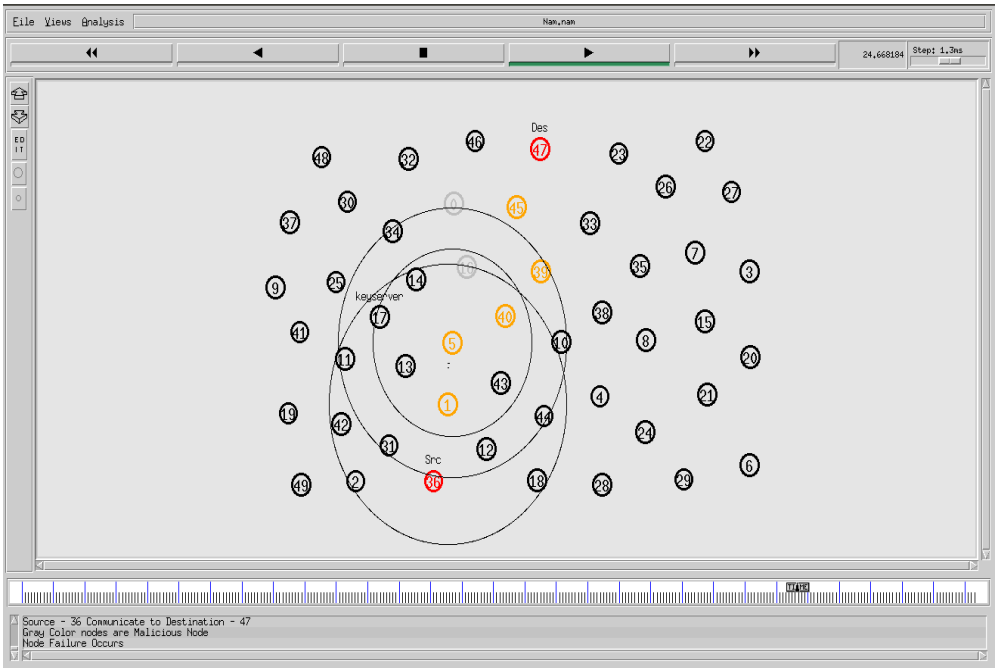

Figure 5: Source to Destination communication via trusted path

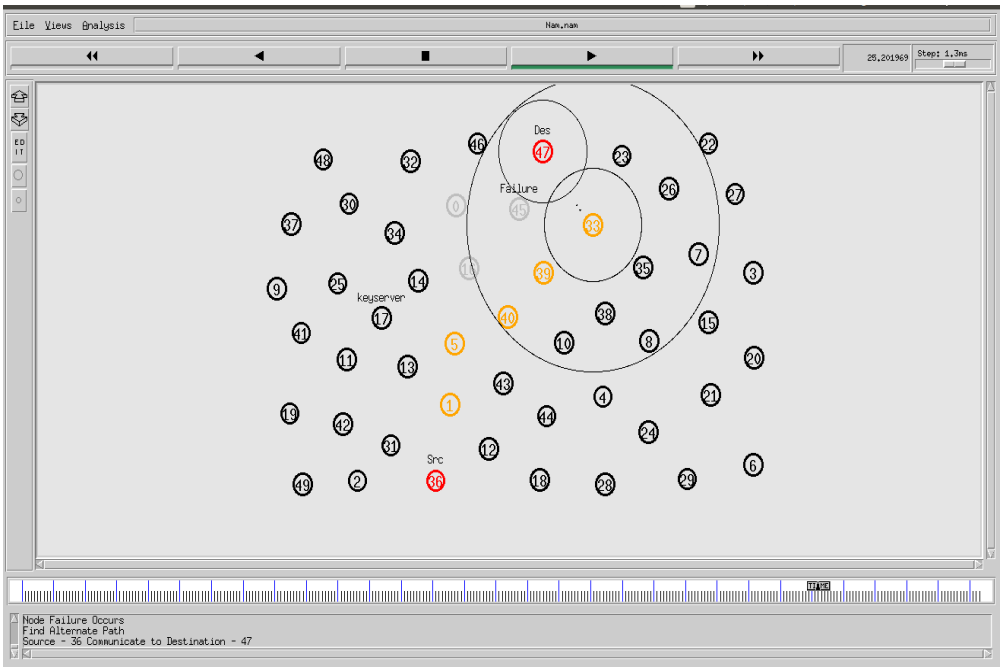

Figure 6: Alternate path selection when node failure occurs

B. Performance Analysis

The analysis is done by comparing the throughput of MANET security with or without trust management.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

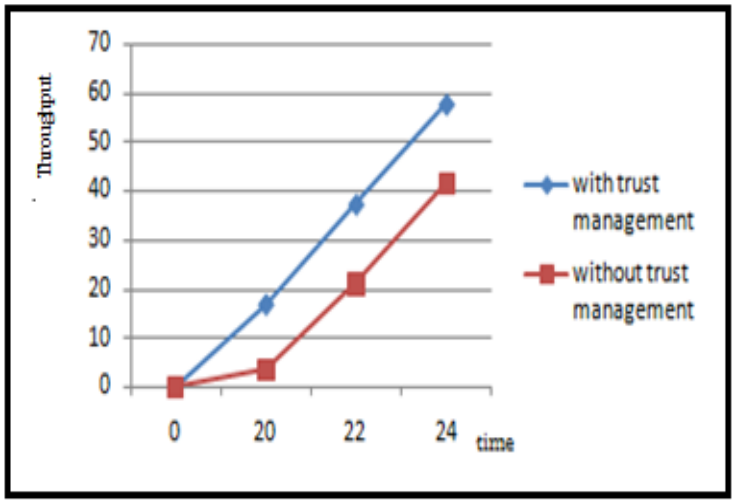

Figure 7: Throughput Comparison

The Figure 7: shows the comparison of throughput by including and excluding trust calculation into the given network. The graph obtained after introducing the trust management is higher that of one which is calculated without trust management.

V. CONCLUSION AND FUTURE WORK

In MANET, the nodes are constantly moving and have no fixed topology. The proposed trust management method improves the MANET security. Malicious nodes in the network are detected by calculating trust value of each node. It monitors single node failure and find the most trusted next node of the failed node in the route. Key server validates when a new node enters into the network.

The method is inefficient to detect multiple node failure. So future work extends to detecting multiple node failure in the routing path and establishes an alternate path.

REFERENCES

[1] Zhexiong Wei, Helen Tang, F. Richard Yu, Maoyu Wang, and Peter Mason, "*Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning*", IEEE Transactions on Vehicular Technology, Vol. 63, No.9, November 2014.

[2] G.Rajkumar, K.Duraiswamy, *"Streamlined Short Alternate Path Protocol for Mobile Ad hoc Networks",* 2013 IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN 2013).

[3] Pallavi Khatri, "*Using Identity and Trust with Key Management for achieving security in Ad hoc Networks",* IEEE 2014.

[4] Aarti, Dr. S. S. Tyagi, "*Study of MANET: Characteristics, Challenges, Application and Security Attacks",* International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

[5] K.Seshadri Ramana "*A Survey on Trust Management for Mobile Ad Hoc Networks***",** International Journal of Network Security & Its Applications (IJNSA), Volume 2, Number 2, April2010.