A NOVEL SECURITY FRAMEWORK USING TRUST AND FUZZY LOGIC IN MANET

Manoj V[1], Mohammed Aaqib [2], Raghavendiran N[3] and Vijayan R[4]

[1,2,3] MS Software Engineering, School of Information Technology and Engineering,
VIT University, Vellore.
manojv1991@gmail.com
aaqibrayan@gmail.com
sriragav.2009@gmail.com

[4]Assistant Professor(Senior),VIT University, Vellore
rvijayan@vit.ac.in

ABSTRACT

Wireless communication is vital during natural calamities, disasters and military operation. In the past few decades, security in the military operations is exposed to vulnerabilities like sniffing the information and modifying the data causing havoc in military camps. Consequently military applications required a secure way to exchange the data and stay away from enemy intrusion. Recent trends in military operations need a portable way of communicating between the units, quality of service and security to be full-fledged. However, in Manet mobile entities are prone to various security attacks due to dynamic changing topology, open medium and inhibited by limited energy, bandwidth and computational power. The paper addresses the security issues by incorporating the concept of trust and certification authority to combat the misbehaving entities. Certificate authority employs fuzzy based analyzer to distinguish between trusted and malicious behavior of nodes by distributing the certificates only to the trusted nodes and detecting the misbehaving node. The proposed scheme is more secure, reliable and aids to improve the security in military operations.

KEYWORDS

Trust, MANET, Security in Military Application, Fuzzy Logic, Security, Security in MANETs, Malicious node detection.

1. INTRODUCTION

Mobile Ad hoc Network (MANET) is a decentralized, infrastructure-less network where wireless nodes move arbitrarily. Trust is defined as a degree of belief about the behavior of other entities. Establishing trust relationships among participating nodes is vital that their trust value or reputation will be hurt by non-cooperative or destructive behavior. Motivation towards trust is from assistance in decision-making to improve security and robustness, Misbehavior detection, Adaptation to risk.

2. DESIGN CHALLENGES IN MANET

MANET exhibits unique features like open medium, dynamic topologies, bandwidth constrained, variable capacity links, energy constrained operation, limited physical security MANETs hence attracted by the attackers. The nodes in the MANET are vulnerable to all kinds of attacks launched through compromised node. Constraints in bandwidth, computing power, and battery power in mobile devices can lead to application specific trade-offs between security and resource consumption of the device.

DOI : 10.5121/ijdps.2012.3124

MANETs must provide various levels of security guarantees to different applications for their successful deployment and usage. However, due to their wireless links and lack of central administration, MANETs have far greater security concerns than conventional networks. It is easy for attackers to eavesdrop the messages since there is no physical connection. Without a security scheme in place, an intruder can easily participate in routing packets. Therefore, it can directly attack the network by dropping packets, tampering with packets, injecting false packets or flooding the network. As a result, it is possible to launch sophisticated wormhole, man-in-the-middle and Denial of Service (DoS) attacks with ease, or to impersonate another node. Security protocol designers for MANETs face technical challenges due to severe resource constraints like memory size, openness to eavesdropping, lack of specific ingress and exit points, high security threat, vulnerability, unreliable communication, and rapid changes in topologies or memberships because of user mobility or node failure

3. STUDY BACKGROUND – MILITARY APPLICATION

Military rescue operations, mine identification operations are typical environments in present military condition. In War fields soldiers rely upon wireless medium to communicate data from airways to stations and to exchange conversations among them. Armed forces badly need to track down the spots of their allies to transmit information. Many security loopholes marked the decline of the powers of Japan and Germany during World War II. The extensive technologies developed in United Nations were effective enough to break the codes of Hitler messages; most of them coded by Enigma or German "Fish Codes" and in no time, German forces were succumbed. Military zones with high secret codes, signal intelligence, missile warning systems and mobility factors demands a strong security. To improve security in military zones, the proposed security scheme provides two levels of security by incorporating trust based data exchanges and fuzzy based analyzer to detect the misbehaving nodes.

Mobility is a critical factor in military applications as missions will start at certain co-ordinate and will end up at the other and tracking the positions of soldiers is most compelling. Self formation of units can be deployed without forming any infrastructure. Nodes may be soldiers or vehicles or unmanned jets. Delivery of messages, quality of service, voice-recordings, video-tapes and images are usual messages in the battlefield to be exchanged with soldiers and other field units. Delay of messages, delivery of erroneous messages and dropped messages can be disastrous. The proposed scheme employs Certificate Authority for reliable transfer of messages when it reaches the destination. When number of entities act in such applications, it is likely that false behaving entities can intrude into the network, steal the data and anonymously modify the messages. Identifying malicious nodes and isolating them without harming the messages will add credits in delivery of reliable messages. Close investigation of such warfare and military applications, requires multi-level security to combat the security vulnerable.

4. RELATED WORKS

4.1 Watchdog Mechanism

The watchdog mechanism, based on a node supervising all its local neighbors, is one of the basic security mechanisms. It is able to detect both malicious attacks and selfish behaviors without significant overhead. In this paper [1] watchdog component monitors its neighbor nodes for behavior. The Watchdog component is responsible of monitoring the received messages with the purpose of making sure that it has forwarded the message without alteration. When intermediary nodes forward the message to its neighbor, it can also verify that the next hop correctly retransmit the message. With the observed behavior, the node can be termed as trusted or malicious.

4.2 Trust Management Framework

The proposed trust management framework in [2] includes Trust agent, Recommendation agent and the Combiner. In this paper the Trust agent derives trust levels from events that are directly experienced by a node. The Recommendation agent shares trust information about nodes with other nodes in the network. The Combiner computes the final trust in a node based upon the information it receives from the trust and recommendation agents.Trust Agent in the proposed framework resides on every node and perform the task of trust derivation, quantification and computation. The recommendation agent sends its own recommendations to other requesting nodes. The Combiner receives trust values from the Trust agents and Recommendation agents. Based on the obtained trust values, final trust computations are done.

4.3 Energy Considerations

The energy of mobile nodes in ad hoc networks is powered by batteries with limited energy. Hence the nodes with minimal energy can turn into selfish nodes. In this research work [3], the proposed scheme discriminates the selfish and the malicious nodes. The total expenditure at a node is calculated by a devised formula considering the energy spent on transmission and the reception of data packets, acknowledgments and on other nodes.

4.4 Fuzzy Logic Based Trust Levels

Fuzzy logic based functions are approximate results rather than fixed and exact. Fuzzy logic variables may have trust values that range in degree between 0 and 1. In the proposed scheme [2] trust decision is based on fuzzy logic. If the evaluated trust is greater than or equal to the threshold trust, then that particular node is called as a trustworthy, else it will be treated as untrustworthy and excluded from all future network operations. Depending upon the grade of trustworthiness the node can be included in the network operations and may be assigned different duties viz. send both the data and routing packets.

Fuzzy trust is represented [4] by the trust level that ranges over the set of values from very untrustworthy to very trustworthy levels. It enables to specify a range for a given trust level instead of giving it a particular discrete value. Trust levels ranging from very untrustworthy, untrustworthy, medium trustworthy, trustworthy, very trustworthy, unknown based on fuzzy logic.

4.5 Packet Modification

Packet modification by malicious nodes is a security threat in MANET. The overview of SAODV protocol [5] provides security mechanisms based on non-invertible hash functions and public key cryptography. The Route Request packet (RREQ) travels through the network until an intermediate node, which knows the path towards the destination, is met or until the destination node is reached. In SAODV, hash chains are applied for the hop count authentication so that each node, at every hop, can verify that the hop count metric was not maliciously decreased.

Receiving a message, a node verifies its authenticity, checking the digital signature content, decrypted through the public key of the node originating the message, is equal to the fields of the received packets. In this way, if an intermediate node modifies the message content, this modification can be detected by the next node receiving the message and the packet can be discarded.

4.6 Security Attacks[9]

4.6.1 Attacks using Modification

Modification is a type of attack when an authorized party not only gains access to but tampers with an asset. For example a malicious node can redirect the network traffic and conduct DOS attacks by modifying message fields or by forwarding routing message with false values.

4.6.2 Attacks using Impersonation

There is no authentication of data packets in current ad-hoc network, so a malicious node can launch many attacks in a network by masquerading as another node i.e. spoofing. Spoofing is occurred when a malicious node misrepresents its identity in the network such as altering its MAC or IP address in outgoing packets and alters the target of the network topology that a benign node can either.

4.6.3 Attacks through Fabrication\

Fabrication is an attack in which an authorized party not only gains the access but also inserts counterfeit objects into the system. In MANET, fabrication is used to refer the attacks performed by generating false routing messages

4.6.4 Gray Hole Attack

Gray hole attack can advertise its route as a valid path with the motivation of intercepting the packets. The packets that pass through the attacked node are dropped with certain probability. These attacks are difficult to spot because it exhibits different behavior to different nodes. It drops packets forwarded from a particular node and forwards the packet from different set of nodes. The parameters like packet modification, packet drop can greatly recognize this type of attacks.

4.6.5 Worm Hole Attack

A wormhole attack follows the tunnelling process. Group of nodes collaborate to encapsulate and exchange messages between them. No packets are allowed in the path leading to short-circuit of normal flow of packets. This type of forwarding can eat the energy of the nodes at a large extent. Parameters likely involved here are Packet delay and Energy.

4.6.6 Black Hole Attack

In black hole attack, the node advertises as a valid path to the destination and intercepts every packet without forwarding and can generate fake information. The possible changes the attack can accomplish is to modify the packet or can delay the packet without forwarding.

4.6.7 Jellyfish Attack

This type of attack can enter into the forwarding group and can delay the packets unnecessarily for a specific time and then forwards the packet. This can decrease the performance of the network and increases the traffic in flow of packets.

4.6.8 Denial of Service Attacks

Denial of service attacks aim at the complete disruption of the routing function and the entire operation of the ad-hoc network. Specific instances of denial of service attack include the routing table overflow and the sleep deprivation torture. In a routing table overflow attack the malicious node floods the network to consume the resources. Parameters of DoS are route request packet modification and re-routing.

4.6.9 Rushing Attack

An attacker node which receives a “route request” packet from the source node floods the packet quickly throughout the network before other nodes which also receive the same “route request" packet can react. Nodes that receive the legitimate route request packet assume those packets to be the duplicates of the packet already received through the attacker node and hence discard those packets. This attack is based on route request packet duplicates and modification as parameters.

4.6.10 Resource consumption Attack

In this attack, a malicious node deliberately tries to consume the resources e.g. battery power, bandwidth, etc of other nodes in the network. The attacks could be in the form of unnecessary route request control messages, very frequent generation of beacon packets, or forwarding of stale information to nodes. The parameters like packet modification, energy can greatly recognize this type of attacks.

4.7 Certificate Authority

A Novel Approach for Providing Security in VANET uses Certificate Authority [6]. Central authority (CA) nodes are responsible for assigning public and private keys to the requesting nodes in the network. These nodes are assigned by the service provider based on their type. Source nodes request available CA node for transmission with the destination node. Destination node receives message from the source node. Message transmission process with source node, destination node and CA is explained in [6].

To resist against attacks from outsider nodes, a hop-by-hop authentication protocol is proposed [7]. It authenticates packets at every hop using a CA based approach and drops any packets that originate from outsiders. Integrity factor is added to secure the network. Certificate authority scheme will increase the security to tackle both internal and external attacks. The scheme consist of three components Monitoring Routing cum forwarding (RCF) behavior, Certificate revival, Certificate revocation.

4.8 Cryptographic Algorithms

One of the foremost challenges is the mismatch between the energy and performance requirements of security processing. In this paper [8] energy consumption of the security protocols and cryptographic algorithms are analyzed. Symmetric algorithm use same key for encryption and decryption. Asymmetric algorithm uses public and private key for encryption and decryption. Hash algorithm takes a message of arbitrary length and outputs a fixed-length hash number representative of the message. Even a minor change in the original message can result in the computation of a different hash value.

Asymmetric algorithm consumes energy for key generation, signature and verification. RSA utilizes minimal energy for verification, while Digital Signature Algorithm and Diffie Hellman consume more energy. Hash algorithms are the least complex of the cryptographic algorithms and should intuitively incur the least energy cost. SHA comes at higher cost than MD4 and MD5.

5. Component of Proposed Framework

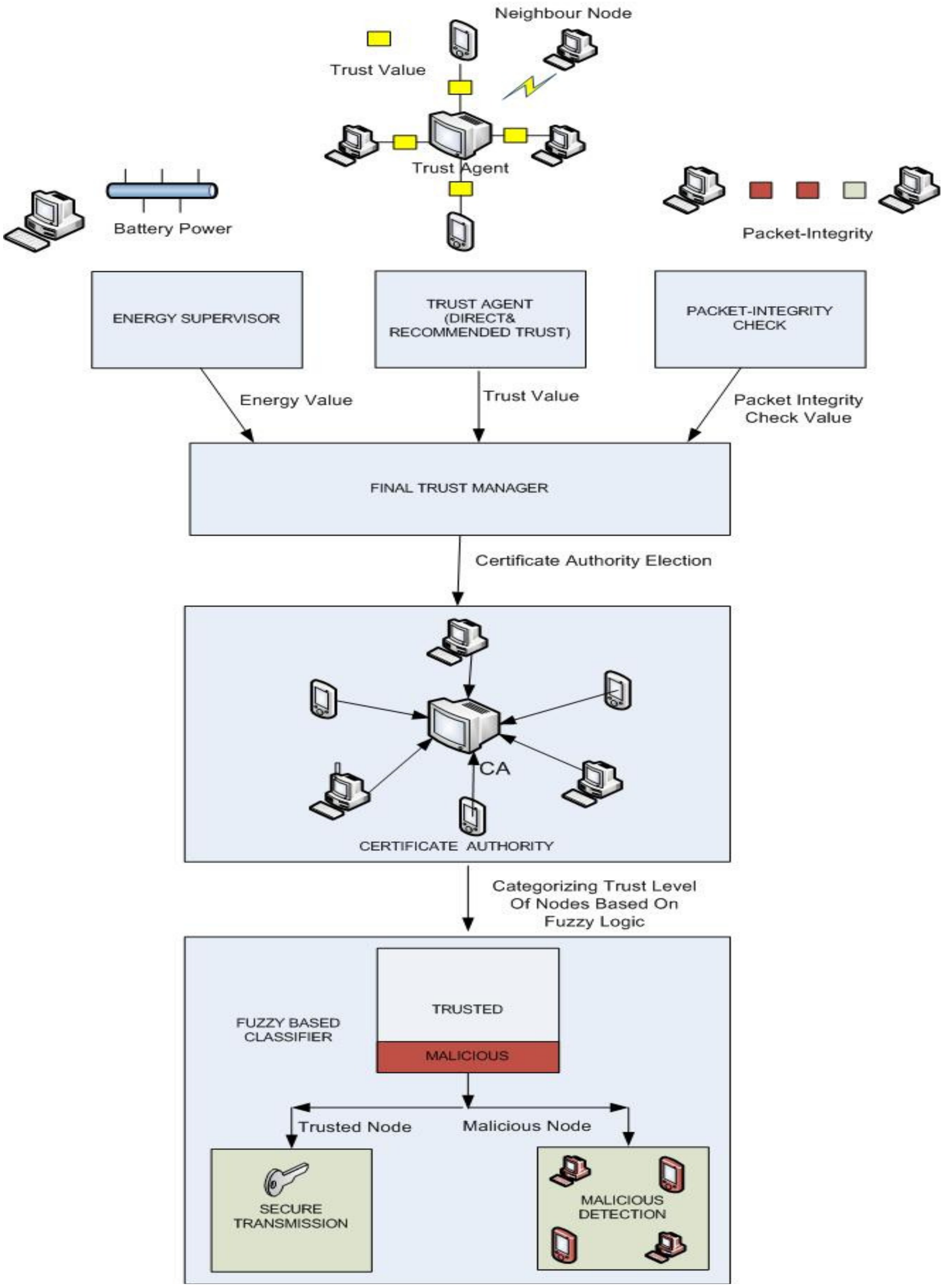


Figure 1. Proposed Security Framework

5.1 Energy Auditor

In Mobile Ad hoc network, the nodes are spending some energy for receiving data packets and some amount of energy for forwarding the packets to neighbor nodes. Initially they have maximum energy that means nodes with full battery capacity. After the communication starts energy consumption also starts. This consumption of energy is more for trusted nodes because, they have to receive as well as forward the packets to its neighbors. But is case of selfish nodes energy utilization is somewhat low, they only receive data packets, they won't forward packets to neighbors. Energy calculation requires initial node configuration. In node configuration initial energy, ideal power consumption, receiving power consumption, transmission power consumption all these details should be specified.

In wireless ad hoc networks energy resource is critical for healthy behavior of the nodes. Due to limited resource availability, nodes behave selfishly by saving the battery power without forwarding the packets to the neighboring nodes. Energy Supervisor monitors the energy spent by each node for sending and receiving the data and control packets [3]. Number of packets forwarded by a node and number of packets received by a node declines the battery power rapidly and affects the trust value of each node, processed by energy supervisor (E_{value}).

5.2 Trust Agent

Direct and recommended trust [2] values are obtained by the trust agent periodically if the trust of node is required. Trust value (T_{value}) is a combination of direct and recommended value from its one hop neighbors in its range.

5.2.1 Direct Trust

Direct trust calculation comes under direct observation of neighbors. In this proposed scheme, every node in the network monitors the behavior of its neighbors, and if any abnormal action is detected, it invokes an algorithm to determine direct trust value. This module monitors neighbor nodes by passively listening to their communication for detecting dropped packet, delayed packet, forwarded packet. Every node in the network monitors the behavior of every other neighbors using watchdog mechanism to check whether neighbor really forwards the packet or drop them. By default all the nodes while communicating with other nodes the direct trust value of all the communicating nodes are calculated and stored in the trust table of corresponding node with field name like node index, direct trust value and one more total trust value of the corresponding node.

5.2.2 Recommended Trust

5.2.2.1 Algorithm for calculating Recommendation Trust

Obtaining Indirect Trust on Y from N

1. Node X sends RTREQ to node(s) N.
2. *If* node X has direct trust value on Y, then it will reply back with RTREP.
3. *Else If* X does not have direct trust value record it will discard the RTREQ
4. After receiving RTREP reply from neighbors consider the trust value of the node with maximum direct trust value by applying fuzzy logic.
5. Integrate all the obtained RT value from neighbors to calculate the indirect trust value

where

RTREQ is Recommendation Trust Request.
RTREP is Recommendation Trust Reply

The task of recommendation agent is to collect or request the trust related information of target node from the neighbouring nodes. The source node will broadcast the recommendation request packet to all its neighbouring nodes. From the reply packets, fuzzy logic is applied to the direct trust value of all the replied neighbours. The node with maximum trust value is considered for evaluation of recommendation trust value.

5.3 Packet Integrity Check

The intermediate node that modifies the message content is detected and the packet can be discarded thus maintaining the integrity of the packet. PIC_{value} is a positive value at initial stage and if there is modification of request packets by a node its PIC_{value} will be decreased. Each node generating a message includes a digital signature generated through its private key and all fields with the exception of the hop count field. In request packets hash chains are applied for the hop count field so that each node, at every hop, can verify that the hop count metric was not maliciously decreased [5]. If a node receives a message, it verifies its authenticity, by decrypting using the public key and the digital signature of the node that originated the message to match with the fields of the received packets. In this way, if an intermediate node modifies the message content, modification can be detected by the next node receiving the message, the packet can be discarded and its PIC_{value} will be decremented. In our proposed scheme RSA algorithm is implemented as it performs signature verification efficiently and incurs least cost compared to other asymmetric algorithms. The huge discrepancy in the energy costs of sign and verify operations in RSA [8] results from the significant difference in the sizes of the keys employed.

5.4 Final Trust Manager

The final trust manager is invoked to calculate the final trust value of target node with Energy value, Trust value and Packet-Integrity value. Based on these obtained values absolute trust value of each node is computed and a timeout value is assigned. Final trust manager also generates Node Trust Table (NTT) with the records Node id, trust type, trust value and trust timeout. Once the trust values of the node gets expired the CA node requests Final Trust Manager to compute the trust value. Each node maintains its NTT and whenever Final Trust Manager is invoked to compute trust, the table gets updated. Final Trust (FT_{value}) is calculated as follows

$$FT_{value} = E_{value} + T_{value} + PIC_{value} \quad (1)$$

Where,

FT_{value} = Final Trust Value of Node

E_{value} = Energy Value of Node

T_{value} = Trust Value of Node

PIC_{value} = Packet-Integrity Value of Node

5.5 Certificate Authority

Node with the maximum trust value is elected as Certificate Authority by incorporating CA election algorithm. Other nodes request the CA node to acquire certificates for data exchange [6]. CA nodes evaluate the trust value of the requestor node by obtaining the trust value from the Final Trust Table. Based on the trust value certificates are issued only to the trusted nodes for secure transmission and malicious nodes are isolated from the network. Certificates [7] are issued to the trusted nodes with a timeout value and once the timeout value expires the certificates have to be renewed. Any trusted node with the highest trust value will be elected as CA. A single mobile node functioning as a CA will bring the entire MANET to a halt if it moves out of its range and also act as a single point of failure if it becomes compromised. Replacement CAs is used in the proposed approach to prevent this security bottleneck.

5.5.1 Certificate Exchange Algorithm

After the source and destination nodes obtain certificates from CA, it is eligible for packet transmission. Source node uses public key to hash the packet and forwards it to the destination. Only the destination node can verify the packet using its private key. Hash algorithms are least complex of cryptographic algorithms and should incur least energy cost. In this scheme MD4 is used to hash the packet .Once the timestamp value in the certificate expires, the node has to request CA node for the renewal of certificates.

Table 1.Certificate Exchange Algorithm

1. Generate Shared Key SKac . 2. Source node request CA E[CREQ(SID,DID,FTValue)SKac] 3. CA node decrypts CREQ looks for SID in ID repository. 4. IF(SID==ID)THEN 5. CA node verifies for SID and checks for DID in its range. 6. Generate PUa,PRa, PUb,PRb, SKbc, CERT A=SID,PRa,PUa,FTvalue,TS. CERT B=DID,PRb,PUb,FTvalue,TS. 7. CA sends CREP as E[(CERT A)SKac] to source node A. 8. CA sends E[(CERT B)SKbc] to destination node B. 9. ELSE DISPLAY("Transmission cannot be granted").	Where PUa,PUb = Public Key of node A and B. PRa,PRb = Private Key of node A and B. SKac = Shared Key of Source and CA. SKbc = Shared Key of Destination and CA. SID,DID = Source and Destination ID

5.5.2 Message Transmission – ISAKMP

ISAKMP format provides a consistent framework for security association, key management and authentication which is independent of the key generation technique, encryption algorithm and authentication mechanism. Certificate exchanges and Authentication in our proposed model as shown in Fig 3 follows the procedures as defined in ISAKMP. Before the actual transmission is started among source node, destination node and CA node ISAKMP process is invoked. Source sends a request message to CA node encrypting it with the shared key SKac. On receiving this request the CA node decrypts the message and first checks whether the source and destination nodes are valid. CA node generates CERT A and CERT B, encrypts it with shared keys SKac, SKcb and forwards it to the source and destination nodes. Destination node decrypts and verifies CERT A, CERT B and generates Nonce N1 only if certificates are valid and sends to source node. Source node decrypts and verifies CERT A, CERT B, N1 and generates Nonce N2 only if certificates are valid. Data packet exchanges are initiated for secure transmission with CERT A and CERT B.

5.6 Fuzzy Based Analyzer

Trust level represents a node's behavior for reliability where the positive experiences increase the trust level of the node and negative experiences decrements the trust level. Fuzzy logic provides ability to handle uncertainty and imprecision effectively. Fuzzy logic based algorithm for trust has been devised and it is applied to the calculated trust value of the nodes. Trust values are computed based on E_{value} ,T_{value} , PIC_{value} produce $FT_{value.}$ These values are treated as fuzzy input variables and the Fuzzy logic based algorithm marks the nodes as either trusted or malicious. Fuzzy logic based algorithm will be called when the nodes request Certificate Authority (CA node) for certificates to exchange data packets. A two way Fuzzy based analyzer has been designed based on trust values, either to be trusted for data exchanges or marked as malicious if it falls below a Critical threshold and its isolated from the network. [Table 1] categorize the trust levels based on fuzzy theory of computation [4].

5.6.1 Fuzzy Table

Table 2. Fuzzy Discrimination

Fuzzy levels	Trust Values	Semantics
1.very high	0.8 to 1	Trustworthy
2.high	0.6 to 0.8	Trustworthy
3.medium	0.4 to 0.6	Trustworthy
4.low	0.2 to 0.4	Untrustworthy
5.very low	0 to 0.2	Untrustworthy

5.6.2 Fuzzy Logic Based Algorithm For Trust

Fuzzy inference rules are given for categorizing the nodes based on trust levels

Table 3. Fuzzy Rules

1. IF trust value is VERY HIGH THEN node is TRUSTED
2. IF trust value is HIGH THEN node is TRUSTED
3. IF trust value is MEDIUM THEN node is TRUSTED
4. IF trust value is LOW THEN node is MALICIOUS
5. IF trust value is VERY LOW THEN node is MALICIOUS

A node request CA node for certificates to perform data exchange, now Fuzzy Based Analyzer is invoked. Fuzzy Based Analyzer verifies the trust value of the requesting node and performs a look up in the fuzzy table for the fuzzy trust value. Fuzzy Based Analyzer runs the algorithm to determine the node as TRUSTED or MALICIOUS. Fuzzy Based Analyzer works under complete control of Certificate Authority node. If the CA node finds a requesting node as malicious an alarm is generated to intimate malicious node to all the trusted nodes in its range.

This makes the network secure by detecting and isolating the malicious node and prevent them from performing any activity in the range.

5.7 Secure Transmission

The proposed scheme is made secure by incorporating trust levels and Fuzzy Based Analyzer for Certificate Authority. Fuzzy Based Analyzer performs the defined steps and if the requestor node is TRUSTED then CA node generates the certificates and sends it to the requestor node. Nodes with the fuzzy values as VERY HIGH, HIGH, and MEDIUM fall in the TRUSTED category. Now with help of the acquired certificate the TRUSTED node can exchange the data packets. Certificates are issued by the CA node with a timeout value and once the timeout value of the TRUSTED node expires it has to request the CA node for the renewal of certificates to transmit data packets.

5.8 Malicious Detection

Nodes with the fuzzy values as LOW, VERY LOW are marked as MALICIOUS. Fuzzy Based Analyzer invokes the Fuzzy logic based algorithm to detect the malicious nodes. CA node denies the certificate to the MALICIOUS nodes preventing them from participating in the network activities. An alarm is generated by the CA node to indicate the node’s malicious behavior to other trusted nodes in its range thus isolating the less trusted nodes and building a secure system. No suspicious and misbehaving nodes can cause vulnerabilities and threats to the proposed scheme.

6. Simulation Analysis And Results

Qualnet5.0 network simulator is used to simulate a wireless network with AODV protocol. Figure 2 shows a scenario with 6 nodes and the traffic flow among them. These nodes are labelled, ranging from Node 0 to Node 6.Constant Bit Rate (CBR) traffic is set. The simulation detects the malicious nodes based on computed trust values.

The metrics to evaluate the trust of each node are packet forward ratio, packet drop, packet delay. Experimental simulation is based on these parameters and node is marked as trusted and malicious based on threshold value. In this scenario trust value of node 2,3 is below the threshold and is marked as malicious and no certificates can be acquired. Certificate Exchange is through ISAKMP security model.

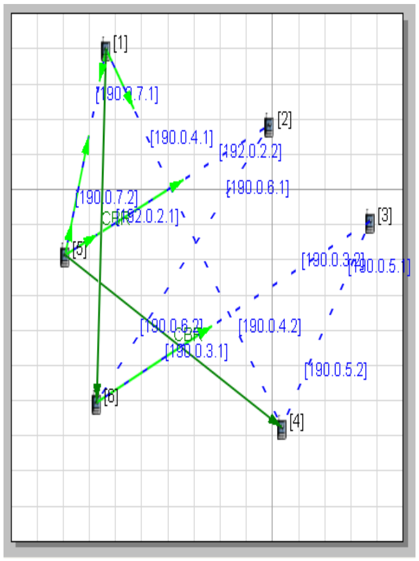
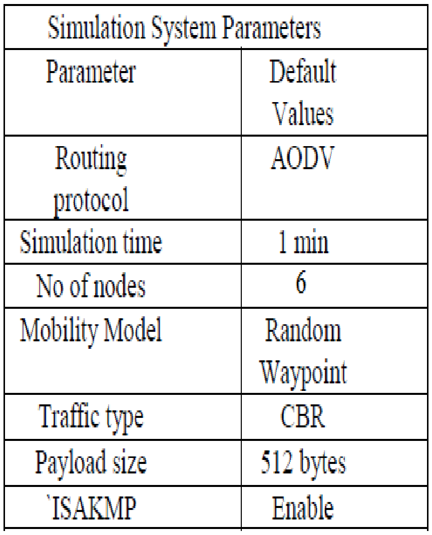


Figure 2. Scenario with 6-nodes.

Table 3. Simulation Parameters.



Simulation System Parameters	
Parameter	Default Values
Routing protocol	AODV
Simulation time	1 min
No of nodes	6
Mobility Model	Random Waypoint
Traffic type	CBR
Payload size	512 bytes
`ISAKMP	Enable

7. Comparative Study

Test cases explain how the proposed framework works with minimum number of nodes (6 nodes) and maximum number of nodes (12 nodes). The graph depicts the probability of detection of malicious nodes of the proposed framework.

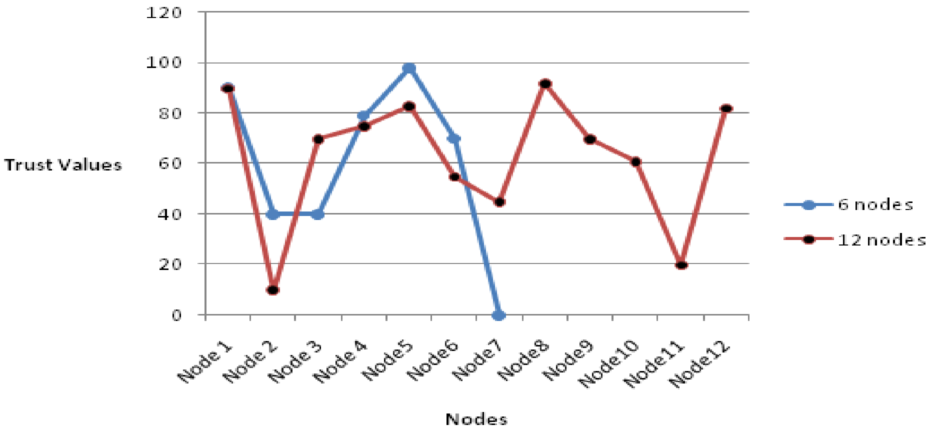


Figure 3. Graph showing malicious node detection.

The graph is plotted with two different scenarios (12 and 6 nodes).With the effect to implementation of our framework, Nodes 2,3 in 6 Node model and Node 2,6,7,11 in 12 Node model are marked as malicious and isolated.

A comparative study is made with the existing system to the proposed framework. We have taken existing system that features Direct and Indirect Trust alone for detection of malicious node without Certificate Authority and Fuzzy Logic. Data are collected from the existing system node and the probability of detecting misbehaving nodes is compared with the probability rate of proposed system. A threshold of 70 is set for all the cases and the trust value of the nodes that fall below the threshold are assumed to be malicious.

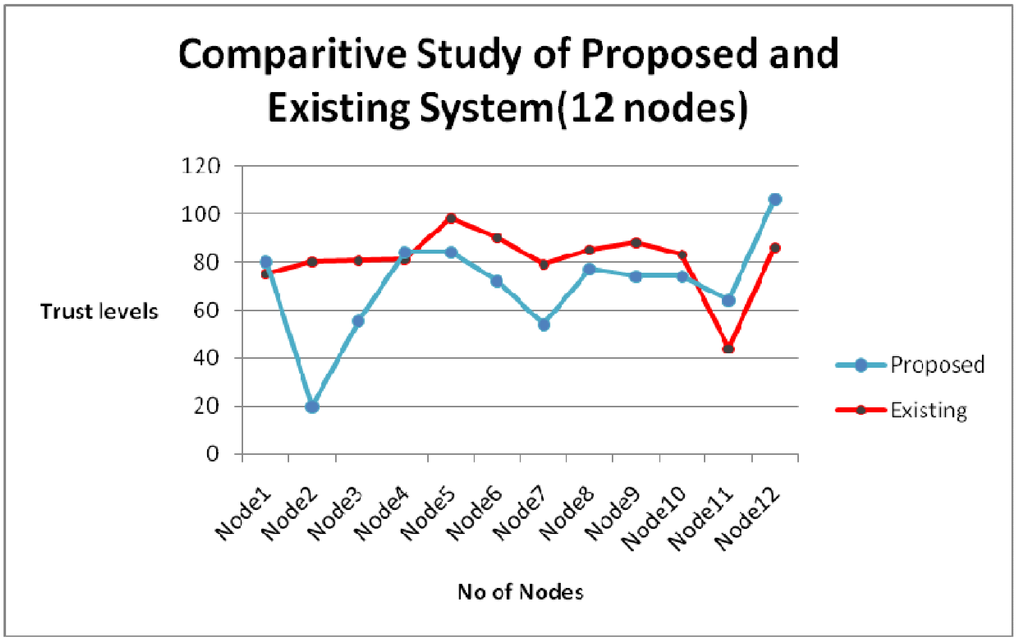
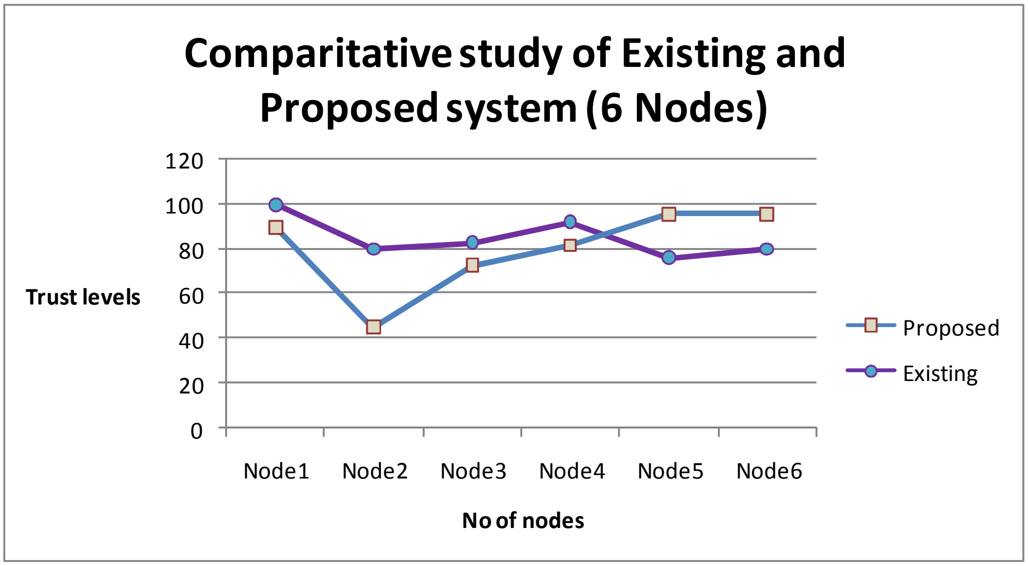


Figure 4. Comparative Study of proposed and existing system(12 nodes)

In this graph for 12 nodes, existing model detects less number of malicious node. In the proposed work, detection of malicious node is higher than that of the existing models.



Fi gure 5. Comparative Study of proposed and existing system(6 nodes)

In this graph for 6 nodes, existing model detect nil malicious node whereas compared to the proposed work, malicious nodes are detected.

The proposed work detects more number of malicious nodes based on the trust value of the nodes if the trust value falls below the threshold set nodes are assumed to be malicious. Comparative study of various test cases with the existing systems and proposed system have shown that proposed system is more accurate and reliable and the probability of detecting malicious node is higher in the proposed scheme.

8. CONCLUSION

MANET consists of various mobile devices with different performance capabilities. Any model proposed for adhoc networks should not impose unrealistic communication and computation requirements. It should be as light as possible. During deployment, security emerges as a central requirement due to many attacks that affects the performance of the ad hoc networks. The proposed work will offer a healthy network by considering the distinctive features like mobility, security and quality of service. Trust is assigned to all the mobile nodes considering the available energy and the nodes are clocked and time lined. Centralized system will monitor the trusted nodes and malicious nodes and assures the certificate exchange is only to trusted nodes. Certificate Authority will protect the data exchange by allowing the trusted entities to participate in the network, isolating the malicious nodes. Trust can alone provide a trustworthiness value of node in a precise way. Fuzzy Logic based on Certificate Authority will provide secure way of message exchanges. Integrated approach of Trust and Fuzzy logic based Certificate Authority will secure the communication

9. FUTURE WORK

- Future work includes analysis of the proposed framework with all other routing protocols to identify the malicious nodes and their efficiency will be compared.
- The proposed framework prevents the system from certain security attacks, in future all the possible attacks will be identified and a new model will be proposed.
- The framework extends to other possible scenarios like PAN, Emergency operation etc.

REFERENCES

[1] Angelo Rossi and Samuel Pierre, (2009)" Collusion-resistant reputation-based intrusion detection system for MANETs", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.11.

[2] V. R. Ghorpade,(2008) " Fuzzy Logic based Trust Management Framework for MANET", DSP Journal, Volume 8, Issue 1.

[3] Mareeswari V, Ramakrishna K and Vijayan R,(2011) "Energy based Trust solution for Detecting Selfish Nodes in MANET using Fuzzy logic", International Journal of Research and Reviews in Computer Science (IJRRCS) , Vol. 2, No. 3.

[4] Ahmad Ridha, Ali Rizvi, Farag Azzedin,(2007) "Fuzzy Trust for Peer-to-Peer Based Systems", World Academy of Science, Engineering and Technology.

[5] Floriano De Rango ,"Improving SAODV Protocol with Trust levels management, IDM and Incentive Cooperation in MANET".

[6] Vijayan.R ,Sumitkumar Singh , (2011) "A Novel Approach for Providing Security in Vehicular Adhoc Network Through Vehicles Present in the Network", International Journal of Advanced Research in Computer Science, Volume 2,no.1.

[7] A.Rajaram and Dr.S.Palaniswami , (2010) "A High Certificate Authority Scheme for Authentication in Mobile Ad hoc Networks", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 5.

[8] Nachiketh R. Potlapally, Srivaths Ravi, Anand Raghunathan,Niraj K. Jha, (2006) “A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols”, Ieee Transactions On Mobile Computing,VOL.5, NO. 2.

[9] G.S. Mamatha and Dr. S. C. Sharma , (2010) “A Highly Secured Approach against Attacks in MANETS “,International Journal of Computer Theory and Engineering, Vol. 2, No. 5.

[10] M Rajesh Babu, Selvan S,(2010) “A Lightweight and Attack Resisitant Authenticated Routing Protocol For Mobile Adhoc Networks”, International Journal of Wireless &Mobile Networks(IJWMN), Vol.2, No.2.

[11] A.Rajaram and Dr.S.Palaniswami , (2010), “Detecting Malicious Node in MANET using trust based Cross-Layer Security Protocol”, International Journal of Computer Science and Information Technologies,Vol 1(2).2010 Pg No:130-137