Journal of Theoretical and Applied Information Technology
20th March 2014. Vol. 61 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DESIGN OF NOVEL SECURITY ARCHITECTURE FOR MANET FOR TRUSTING AND AUTHENTICATION

[1]Mr. J. CHANDRA SEKHAR, [2]DR. R. SIVARAM PRASAD
[1]Acharya Nagarjuna University, Department of CSE, Research Scholar
[2] Acharya Nagarjuna University, Department of CSE, Research Director
E-mail: [1]jcsekhar9@gmail.com, [2]raminenisivaram@yahoo.co.in

ABSTRACT

In MANETs, providing the security for routing and data packets is a big challenge. To overcome those drawbacks in this paper we design Novel security architecture for MANET for trusting and authentication. It provides routing security against jamming attacks, detects stealthy packet dropping attacks, a trust based reputation management system and certificate based authentication system. In first phase, multiple paths are determined based on AOMDV and the end-to-end packet success rate is sent as feedback to the source by the destination. In second phase, based on the method for trust and reputation management is then applied. In third phase, a standard authentication scheme for MANETs is proposed using Threshold Secret Sharing to provide security inside a network allowing only the legitimate users to utilize the network. By simulation results, we show that the proposed architecture reduces the drops due to attack and increases the packet delivery ratio.

Keywords: *Mobile Ad hoc network(MANET),Threshold Cryptography, Secret Sharing, Certificate Authority, Reputation Index.*

1. INTRODUCTION

1.1 Mobile ad hoc network (MANET)

A (Mobile ad hoc network) MANET a self-organizing, independent communication infrastructure is a collection of mobile nodes equipped with both a wireless transmitter and a receiver can dynamically and freely self-organize into arbitrary and temporary ad hoc network topologies to communicate with each other within its transmission range via bidirectional wireless links either directly or indirectly without a central infrastructure. The node relays on other nodes to communicate with nodes outside its transmission range. MANET has its applications in commerce, emergency services, military, education, e-health, the tactical networks, rescue operation, communication and entertainment. [1], [2], Ad-hoc network an autonomous peer-to-peer self-organized networks without an external management has a dynamic network topology due to nodes' mobility and depends on multi-hop routing to forward packets. Communication between nodes with different capabilities and different links without communication infrastructure depends on the energy constraints of the nodes and supports network scalability [3].

1.1 Issues in MANET

Ad hoc networks are subject to various types of attacks ranging from passive eavesdropping to active impersonation, message replay, and message distortion. [4] Security is a critical issue in wireless ad hoc networks due to the vulnerability of the channels and the nodes, the absence of infrastructure, the dynamically changing topology, the bandwidth-constrained links, the energy-constrained operation and the limited computation capability of the nodes. A centralized solution can be easily compromised, leaving the nodes exposed to threats originating from malicious users.[4] MANETs are more vulnerable to security attacks than conventional wired and wireless networks because of their open communication medium, node mobility, lack of centralized security services, dynamic topology, distributed and cooperative sharing of channels and other resources, power and computation constraints and lack of prior security association. Accessing trusted authorities or centralized servers for key management is infeasible for MANETs due to the absence of any infrastructure, frequent mobility, and wireless link instability. And also deploying security mechanisms in MANETs is difficult due to the absence of fixed infrastructure, shared wireless medium, node mobility, limited resources of mobile devices, bandwidth restricted and error-prone communication links, and so on.

As the nodes lack physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks i.e., generally routing protocols considers every node in the network behaves with other nodes and not malicious, attackers can easily compromise MANETs by inserting malicious or non cooperative nodes into the network. [1]

Nodes in MANETs are exposed to malicious entities which tamper and analyze data and traffic analysis by communication eavesdropping or attacking routing protocols. Unlike civil applications, anonymity is required in military applications e.g., soldier communication. Enemies may intercept transmitted packets, track our soldiers (nodes), attack the commander nodes, and block the data transmission by comprising relay nodes (RN) by traffic analysis, thus attacking MANET in battlefield. Anonymous routing protocols in MANETs provide secure communications by hiding node identities including identity and location anonymity of data sources, destinations and route anonymity thereby preventing traffic analysis attacks from outside observers by hindering to trace a packet flow back to its source or destination and to make the node ignorant of real identities and locations of intermediate nodes en route. Additionally, anonymous path is essential between the two endpoints to dissociate the relationship between source and destination and ensure that nodes en route become unaware of endpoints especially in MANETs equipped with location devices may be equipped. [2]

1.2 Various attacks in MANETs

- Sybil attacks
- Resource Consumption Attack
- Rushing Attack
- Black Hole Attack
- Gray Hole attack
- Worm Hole attack

1.3 Authentication

User authentication prevents unauthorized users from accessing or modifying network resources in high-security MANETs. As there is much possibility in capturing the device in a hostile environment, authentication is to be performed continuously and frequently where the frequency relies on the situation severity and the resource constraints of the network. One or more types of validation factors can be used to perform User authentication: knowledge factors, possession factors, and biometric factors. (i)Knowledge factors (such as passwords) and (ii) possession factors (such as tokens) can be implemented easily but can make it difficult to distinguish an authentic user from an impostor if there is no direct connection between a user and a password or a token. (iii)Biometrics technology, generally the recognition of fingerprints, irises, faces, retinas, etc., possibly solves the authentication problem. Individuals can be automatically and continuously identified or verified using this technology by their physiological or behavioral characteristics without user interruption. [5]Authentication between two communicating nodes is provided by (i) symmetric-key cryptosystems where a single key shared between two parties via secure channels, is used to encrypt and decrypt the exchanged information. (ii) asymmetric-key cryptosystems deploys two related keys, the public key and the private key where the public key can be freely distributed, whereas the private key must be kept secret and in a secure location. Each key unlocks the encryption that the other key creates. [3]

1.4 Trust and Reputation in MANET

Trust models are an attempt to formalise trust definitions and are often tied to the establishment of a Public Key Infrastructure (PKI) in MANETs. A trust management and recommendation protocol built upon PGP (Pretty Good Privacy) methods for computing authenticity based on certificates, key bindings, and on trust relationships in which an opinion and evidence driven models are used to represent trust [6].

Reputation and trust are two useful tools that are used to facilitate decision making in diverse fields from an ancient fish market to state-of-the-art ecommerce. Reputation is the opinion of one entity about another. In an absolute context, it is the trustworthiness of an entity. Trust, on the other hand, is the expectation of one entity about the actions of another. For over three decades, formal studies have been done on how reputation and trust can affect decision making abilities in uncertain conditions [7].

1.5 Issues of Trust and Authentication

Following are the issues of Trust management

- Keeping Track of Past Behavior
- Incorporating Data from Different Sources
- Forgetting Reputation over Time
- Secondary Response [8]

A node may easily be stolen and become compromised. Thus, the trust between nodes in ad-hoc networks cannot be guaranteed. Furthermore, this problem may increase the chance to tamper the stolen node. It is also vulnerable since every node in MANET uses radio wave to communicate. It is very hard to detect any node since there is no explicit evidence [9].

If one relies only on self-detecting misbehaviors, one may arrive at a wrong evaluation of trust. In fact, a node that is actually not sending any packets currently cannot detect selfish nodes in its neighborhood. As a consequence, collaboration between neighboring nodes becomes mandatory [10].

The issues of authentication can be summarized as follows:

In biometric authentication processes, two kinds of errors can be made: 1) false acceptance (FA) and 2) false rejection (FR). FAs result in security breaches since unauthorized persons are admitted to access the system/network. FRs result in convenience problems since genuinely enrolled identities are denied access to the system/network, and maybe some further checks need to be done. The frequencies of FA errors and of FR errors are called FA rate (FAR) and FR rate (FRR), respectively. The FAR can be used to measure the security characteristics of the biometric systems since a low FAR implies a low possibility that an intruder is allowed to access the system/network. In tactical MANETs, failure in user authentication might result in serious consequences. Hence, more than one biometric sensor is used at each time period in our system to increase the effectiveness of user authentication [5].

Users of context-based applications would obtain authentication credentials by subscribing to the service. They could subsequently verify that received messages were sent by other subscribers to the service. But if this is done without appropriate precautions, the authentication mechanism would then reveal the identity of the nodes, thus rendering the privacy problem particularly challenging [12].

MANETs are more vulnerable to security attacks than conventional wired and wireless networks. Accessing trusted authorities or centralized servers for key management is infeasible for MANETs due to the absence of any infrastructure, frequent mobility, and wireless link instability. A traditional centralized monitoring technique is no longer feasible in MANETs due to its distributed architecture and changing topology. The complex routing in MANETs and its stringent channel resource constraints leading to energy constraints affects system capacity. In a MANET employing a high-cost anonymous routing in a battlefield, a low quality of service in voice and video data transmission due to depleted resources may lead to disastrous delay in military operations.

In this paper, we propose to design security architecture for MANET which provides routing security against jamming attacks, detects stealthy packet dropping attacks, a trust based reputation management system and certificate based authentication system.

2. LITERATURE REVIEW

Julien Freudiger et al [11] have presented a paper on the problem of self-organized anonymous authentication that is a necessary prerequisite for location privacy. They investigate, using graph theory, the optimality of different cloak constructions and evaluate with simulations the achievable anonymity in various network topologies. They show that peer-to-peer wireless communications and mobility help in the establishment of self-organized anonymous authentication in mobile networks.

.

Erman Ayday et al [12] have developed an iterative malicious node detection mechanism for Delay/Disruption Tolerant Networks (DTNs) referred as ITRM which is a graph-based iterative algorithm motivated by the prior success of message passing techniques for decoding low-density parity-check codes over bipartite graphs. The proposed iterative reputation management scheme far more effective than well-known reputation management techniques like Bayesian framework and Eigen Trust by applying ITRM to DTNs for various mobility models provides high data availability and packet-delivery ratio with low latency in DTNs under various adversary attacks attempting to both undermine the trust and detection scheme and the packet delivery protocol.

Issa Khalil et al [13] have presented SADEC (Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Counter measure), a protocol presenting two techniques based on local monitoring i.e., neighbors maintaining extra information of routing path, and adding some checking responsibility to each neighbor, to detect and isolate stealthy packet dropping attack efficiently. And also, SADEC provides an innovative mechanism to better utilize local monitoring by considerably increasing the number of nodes in a neighborhood that can do monitoring. Baseline local monitoring fails to efficiently mitigate most of the presented attacks while SADEC successfully mitigates them. However, the listening activity for detecting malicious behavior is more complicated due to the presence of multiple channels and multiple radios.

Johann van der Merwe et al [14] have proposed a novel public key management service called Trustworthy Key Management for Mobile Ad Hoc Networks (AdHocTKM) taking the advantages of threshold cryptography and certificate chaining and integrates it with self-certified public keys and self-certificates to yield a key management service that is secure, trustworthy and highly available to users. The paper also proposed a novel cryptographic key issuing protocol allowing negotiation between a single entity and a distributed authority for an implicit self-certified public key, without the authority gaining knowledge of the corresponding private key. This algorithm is called, threshold self-certified public keying.

Zhi Xu et al [15] have proposed the first effort to quantitatively analyze the impacts of node mobility, attack packet rate, and path length on the traceability of two types of well-known IP traceback schemes: probabilistic packet marking (PPM) and hash-based logging. It then presents the design of an authenticated K-sized Probabilistic Packet marking (AK-PPM) scheme, which not only improves the effectiveness of source trace back in the MANET environment, but also provides authentication for forwarding paths. Their simulations results show that AK-PPM can achieve asymptotically one-hop precise, and Present the performance measurement of AK-PPM in MANETs.

From the literature review done, we can observe that there is no fixed security architecture which provides defense against various attacks as well as provide authentication for routing and data packets in MANET.

In this paper, we propose to design security architecture for MANET which provides routing security against jamming attacks, detects stealthy packet dropping attacks, a trust based reputation management system and certificate based authentication system.

3. PROPOSED SOLUTION

3.1 Overview

In this paper we design of Novel security architecture for MANET for trusting and authentication. It contains three phases.

In this First phase, multiple paths are determined based on AOMDV. Among these paths, the end-to-end packet success rate is sent as feedback to the source by the destination. It is estimated based on the packet error rate which is modeled at each network node as a random process for capturing the nondeterministic and dynamic effects of the jamming attack. Based on the estimated packet success rate on each path, the amount of data to be transmitted on each path will be decided.

In this Second phase, based on the method for trust and reputation management is then applied. It uses local and global reputation values which can be adaptively adjusted based on the reports from monitoring nodes.

In this Third phase, a standard authentication scheme for MANETs is proposed using Threshold Secret Sharing to provide security inside a network allowing only the legitimate users to utilize the network. In this algorithm multiple Certification Authority (CA) nodes are selected based on the evaluated reputation index, transmission power and mobility. By making the node aware of the time a close-by CA is out of order, threshold cryptography implementation in the network is enhanced and hence less overhead and faster completion of the authentication process is achieved.

3.2 Phase 1: Estimating End-to-End Packet Success Rate

Initially multiple paths are selected based on the AOMDV. Consider the following example. S is source and D is the destination. S wants to send the packets to the destination and S sends RREQ packets to all its neighboring nodes. The neighboring nodes forward the packets to its neighboring nodes. Finally, destination received the RREQ packets and replay with RREP packet.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

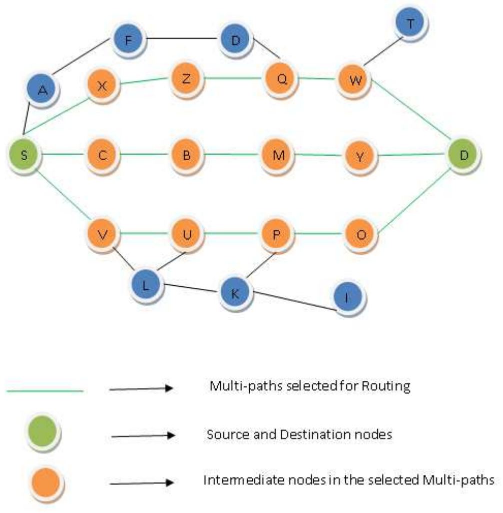
F
D
T
A
X
Z
Q
W
S
C
B
M
Y
D
V
U
P
O
L
K
I
Multi-paths selected for Routing
Source and Destination nodes
Intermediate nodes in the selected Multi-paths

Figure 1: Example for Route Discovery

In the above example, S has multiple paths to send the data to the destination. They are three are available to send the packets to destination.

S → X →Z →Q →W →D
S →C →B →M →Y →D
S →V →U →P →O →D

Among these paths, the end-to-end packet success rate calculated based on packet error rate and sent the calculated end-to-end packet success rate as feedback to the source. The packet error rate is made at each network node as a random process for capturing the nondeterministic and dynamic effects of the jamming attack. This phase is useful estimating and characterizing the impact of the jamming, send the estimated to source as a feedback.

3.2.1 End-to-End Packet Success Rate

$P_{i,j}$ is the end-to-end packet success rate over link (i,j). There are individual jamming strategies for jamming the data transmission. In this paper, the packet success rate is modeled as random process and allows the intermediate nodes to collect the data to characterize the process.

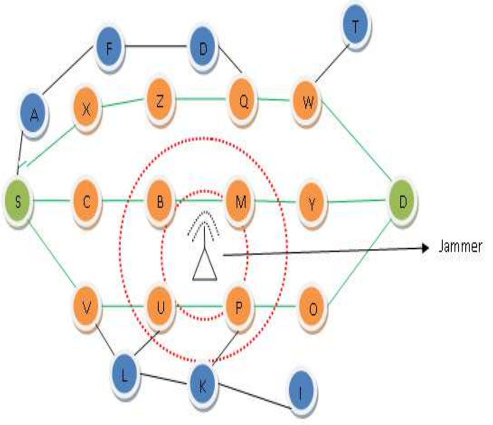

Figure 2: Example for Jamming Attack

The packet delivery ratio (PDR) is computed to estimate the $U_{i,j}(t)$. The time interval is T = [t-T, t]. The time interval is used to update the estimated $U_{i,j}(t)$ values to S. Consider the node C, receives the $R_{i,j}$ number of packets during the time interval T and $V_{i,j}$ is the valid number of packets during the same time interval. The PDR is calculated using the following equation

$$PDR_{i,j} = \frac{V_{i,j}}{R_{i,j}} \quad \text{(Allareat sametimeintervalT)} \quad (1)$$

The above $PDR_{i,j}$ (T) is over the link i, j. The $PDR_{i,j}$ (T) is used to update the estimate the $U_{i,j}(T)$. The memory of the jamming attack history and exponential weighted moving average (EWMA) [17] is used included to provide the significant variation in the estimation of $U_{i,j}(T)$.

$$U_{i,j}(t)=\beta*U_{i,j}(t-T)+(1-\beta)*PDR_{i,j}(T) \qquad (2)$$

In the equation (2), β is a constant weight indicating the relative preference between current and historic samples. We use the EWMA process to update the variance at the end of each update replay period of T_s. Variance is calculated using the following equation [16]

$$U_{i,j}(t) = \beta * U_{i,j}(t - T) + (1 - \beta) * PDR_{i,j}(T) \qquad (3)$$

We use a similar EWMA process to update the variance at the end of each update relay period of T_s. The sampling variance is calculated using the following equation [17]

$$\begin{bmatrix} VR_{i,j}(\mathrm{T_s}) = Var(\mathrm{PDR}_{\mathrm{i,j}}(\mathrm{t - KT, t - KT + T}) \\ \text{where } \mathrm{K} = 0....[\mathrm{T_s/T}] - 1 \qquad (4) \end{bmatrix}$$

In the equation (4), $VR_{i,j}(\mathrm{T_s})$ is intended to capture the variation in the packet success rate over the last $\mathrm{T_s}$. The estimated variance is calculated using the following equation [17]

$$\sigma_{i,j}{}^2(\mathrm{t}) = \alpha * \sigma_{i,j}{}^2(\mathrm{t - T_s}) + (1 - \alpha)VR_{i,j}(\mathrm{t - T_s, t}) \qquad (5)$$

The end-to-end packet success rate ($\mathrm{P_{i,j}}$) is calculated based on the $\mathrm{U_{i,j}(T)}$ using the following equation [16]

$$P_{\mathrm{S,D}} = \prod_{(\mathrm{i,j})\in \mathrm{PA}_{S,D}} \mathrm{U_{i,j}} \qquad (6)$$

In equation (6), $\mathrm{PA_{S,D}}$ is the end-to-end packet success rate for the selected multiple paths. Based on the estimated packet success rate on each path, the amount of data to be transmitted on each path will be decided.

3.3 Phase 2 - Trust and Reputation Management

In this Second phase, trust and reputation management method is applied. The Trust and Reputation method is used to identify sources of attack and malicious node. A node is identified by another node by reliable packet delivery of that node. That is called “trustworthy” of a node.

Reputation is based on the past behavior and time of a node. These past behavior of nodes are stored in the data form in a centralized or in a distributed way. A distributed storage is needed for self-organized networks and there is no need of any centralized reputation authority. A node collects the data based on the interest. Reputation Index is used to store the reputation of the nodes in a tabular format.

Table 1: Reputation Index table

S.No.	Node 1	Node 1	Reputation Index
1	-	-	-
2	-	-	-
3	-	-	-
4	-	-	-

In the above table, the reputation index is calculated by $\mathrm{S_{i,j}}$. $\mathrm{S_{i,j}}$ is the sum of the ratings of individual transactions (Satisfactory Transactions and Unsatisfactory Transactions). The value of $\mathrm{S_{i,j}}$ is calculated using the following algorithm.

1. Start
2. Define $\mathrm{G_i}$ = Global Trust Value
3. $\mathrm{L_i}$ = Local Trust value
4. $\mathrm{S_{i,j}}$ = Sum of ratings of individual transactions.
5. // Calculating the Local Trust Value between the node I, j
6. Node i receives a data packet from node j. If the received data packet is good then the $\mathrm{L_i}$ is 1 and if the received data packet contains any harmful data then it $\mathrm{L_i}$ value is 0.
7. $S_{i,j} = \sum \mathrm{L(j)}$
8. $S_{i,j} = \mathrm{ST(i, j) - US(i, j)}$
9. ST(i,j) = Satisfactory Transactions
10. US(I,j) = Unsatisfactory Transactions
11. Normalize the local trust value
    $N_{i,j} = \dfrac{\max(\mathrm{S_{ij}},0)}{\sum \mathrm{S_{ij}},0}$
12. End

Algorithm 1: Trust and Reputation Management algorithm

Every node has two values one is Global trust value and second one is Local trust value. The local trust value of a node is calculated based on number of packets received between the nodes. If the node gets the malicious data packets then the local trust value be 0 and remaining data packets have 1.

Calculate the Sum of the rating of individual transactions. Normalize the trust value, to aggregate the local trust values.

3.4 Phase 3 - Threshold Secret Sharing

In this phase, multiple Certification Authority (CA) nodes are selected based on the evaluated reputation index, transmission power and mobility. Threshold Secret Sharing is used to provide security inside a network and allowing only the legitimate users to utilize the network.

3.4.1 Multiple Certification Authority

N is the number of secret share holder nodes and T is threshold value. Among the one node in the M should contact with the T number of nodes to become authenticated. When the nodes contact with the T number of nodes then only it authenticated. Authentication between the nodes follows Shamir's threshold scheme [18]. A trusted entity is assigned by the certification authority to share private key among the all members in the group.

When the node needs to authenticated, it should send a message with the share private key in order to create a partial signature. The node sends a message to the all its members of nodes in the group. The message is format is given below

$$a_i = m^{SP_i} \pmod{n} \qquad (7)$$

In the equation (7), m is the message, n is the value from the pairs of the RSA keys of the certification authority and SP_i is the shared secret key of node i.

When the member nodes in the group received the message from the node, which is trying to authenticated, it will send a partial signatures. When the node receives at least T partial signatures, then construct the complete signature for the particular. The node communicates with the other nodes to get those signatures. The Lagrange interpolation is used to create the complete signature from the partial signatures. The complete signatures as follows

$$\prod a_i^{L_i(0)} = \prod m^{SP_i L_i(0)}$$
$$= m^{\sum i \, SP_i L_i(0)} = m^d \pmod{n} = k \qquad (8)$$

In the equation (8), d is the shared private key and using the equation the complete signature is created. But the Certification Authority (CA) nodes are selected based on the evaluated reputation index, transmission power and mobility.

3.4.1.1 Reputation Index:

Reputation Index is the value of the behavior and time of a node. Every node has some reputation about the neighboring nodes. Using the table 1, we will get reputation index values. RI_i is the reputation index of a node i.

3.4.1.2 Transmission Power:

Transmission power is defined as, the estimation of the distance from the node by the power of the signal, when the node received a transmission from another node. TR_i is the sum of the distance between i and all its neighboring nodes. When the nodes have many neighboring nodes then the TR_i value is high. When the several nodes are very near and producing a large amount of interference then the TR_i value is small.

3.4.1.3 Mobility:

A Certification Authority (CA) cannot be defined when the node has high mobility. The parameter M_i is the average speed of node i.

$$M_i = \sum_{i=1}^{m} V_i(j) \qquad (9)$$

In the equation (9), V_i is the velocity of the node J.

$$W_i = c_1 RI_i + c_2 TR_i + c_3 \frac{1}{M_i} \qquad (10)$$

In the equation (10), c_1, c_2 and c_3 are coefficient values. W_i is the weight of the node and it is elected as Certificate Authority (CA).

3.4.2 Enhancing Threshold Cryptography:

Threshold cryptography is very important in MANET, because if the CA is compromised then the security of entire network will be crashed.

Consider a network and it contains N number of nodes. T is the threshold value. These nodes are holding a secret share of the CA's private key.

These nodes are called MOCA (Mobile Certificate Authorities). .A certification protocol called MP (MOCA Certification Protocol) is proposed by Yi and Kravets [19] to provide effective and efficient communication between clients and MOCAs.

In MP, the node sends the Certification REQuest (CREQ) packets to obtain the certification services. Any node in MOCA receives the CREQ packet responds with a Certification REPly Packet (CREP) containing its partial signature. The node wait for fixed period of time for T number of partial signatures to reconstruct the full signature and certification request is completed successfully. If the node did not get the T number of partial signatures, then it will initiate another round of certification requests after a small period of time.

This approach is not effective when the traffic is huge, because it generate fairly large amount of overhead traffic due to many CREQ packets. In order to reduce the overhead, introduced another model is β-unicast.

In this method, the node has enough number of routes then it can use multiple unicast connection instead of flooding. If the node uses more than the routes then it fall back to flooding.

3.4 Total Work Flow

In this paper, initially multiple paths are determined based on AOMDV. End-to-end packet success rate is calculated based on the packet error rate and which is send to sender as feedback by the destination. For each node, the packet error rate is calculated and the packet error rate is to capture the dynamic effects of the jamming attack.

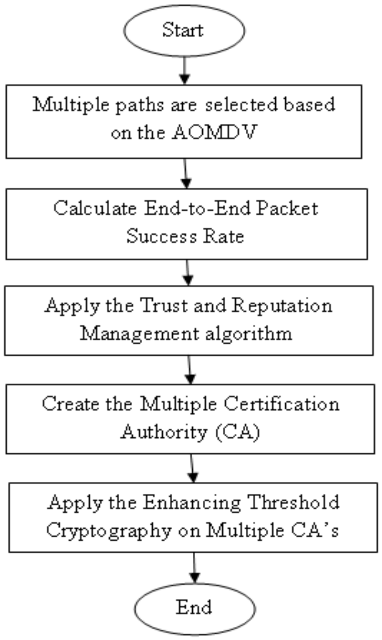
Start
Multiple paths are selected based on the AOMDV
Calculate End-to-End Packet Success Rate
Apply the Trust and Reputation Management algorithm
Create the Multiple Certification Authority (CA)
Apply the Enhancing Threshold Cryptography on Multiple CA's
End

Figure 3: Total Work Flow

Next trust and reputation management method is applied to identify sources of attack and malicious node. Reputation is based on the behavior and time of a node.

In this Second phase, trust and reputation management method is applied. Trust is an important and challenging issue in the security of MANET. Because of lack infrastructure, it is difficult to ensure the reliability of packet delivery nodes. These past behavior of nodes are stored in the data form in a centralized or in a distributed way.

A node collects the data based on the interest. Reputation Index is used to store the reputation of the nodes in a tabular format. It uses local and global reputation values which can be adaptively adjusted based on the reports from monitoring nodes.

To provide the security, a Threshold Secret Sharing is used in MANETs. Multiple Certification Authority (CA) is assigned to any of the node in the group of nodes and that is based on the evaluated reputation index, transmission power and mobility.

Threshold Secret Sharing is used to provide security inside a network and allowing only the legitimate users to utilize the network. Threshold cryptography is implemented to give more security and faster completion of the authentication process.

4. Simulation results

4.1 Simulation Model and Parameters

We use Network Simulator Version-2 (NS2) [14] to simulate our proposed algorithm. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage.

In our simulation, mobile nodes move in a 1000 meter x 1000 meter region for 50 seconds simulation time. We have varied the node speed as 5,10,15,20 and 25m/s. The transmission range is 250 meters. The simulated traffic is Constant Bit Rate (CBR).The numbers of attackers are varied as 1,2,3,4 and 5.Our simulation settings and parameters are summarized in table 2

Table 2: Simulation Settings

Number of Nodes	50
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Speed	5,10,15,20,25m/s
Routing Protocol	NSATA
No. Of Attackers	1,2,3,4 and 5.

4.2 Performance Metrics

We evaluate mainly the performance according to the following metrics.

Average Packet Delivery Ratio:

It is the ratio of the number .of packets received successfully and the total number of packets transmitted.

Resilience:

It is the ratio between number of packets dropped and the number of packets sent.

Average Packet Drop:

It is the average number of packets dropped by the misbehaving nodes.

End-to-End Delay:

It is the amount of time taken by the packets to reach the destination.

We compare our Novel Security Architecture for MANET for Trusting and Authentication (NSATA) with the ITRM [12].

4.3 Results

A. Based on Attackers

In our first experiment we vary the number of attackers as 1,2,3,4 and 5.

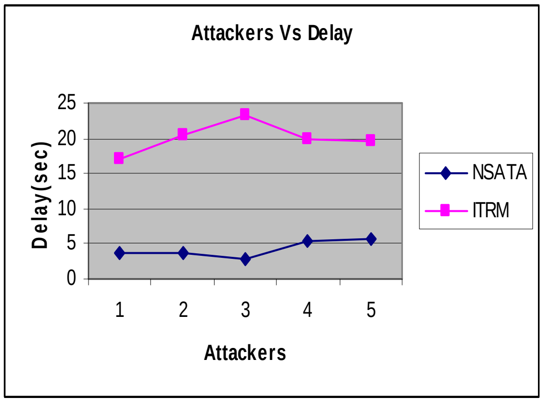

Fig 4: Attackers Vs Delay

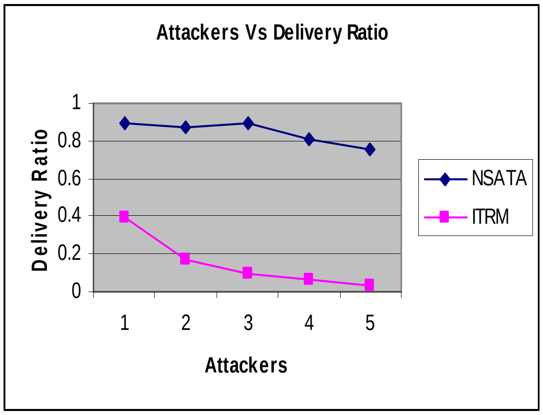

Fig 5: Attackers Vs Delivery Ratio

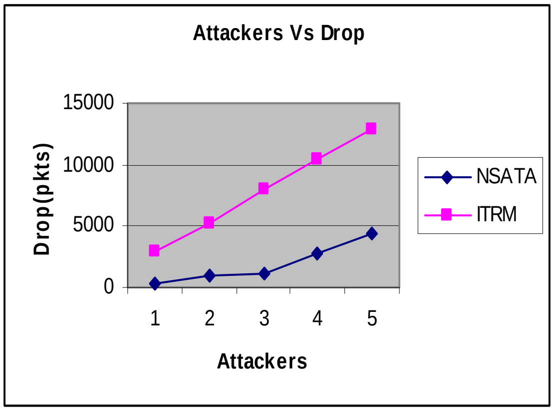

Fig 6: Attackers Vs Drop

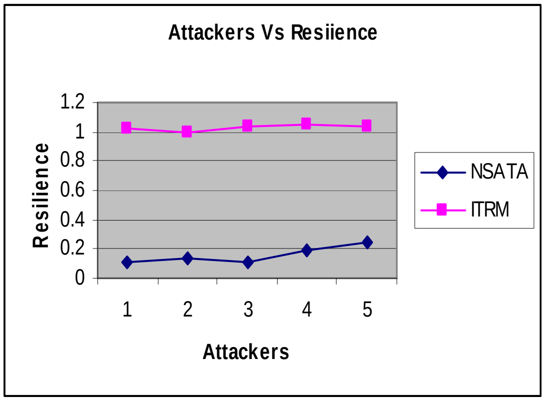

Fig 7: Attackers Vs Resilience

From figure 4, we can see that the delay of our proposed NSATA is 78% less than the existing ITRM protocol.

From figure 5, we can see that the delivery ratio of our proposed NSATA is 82% higher than the existing ITRM protocol.

From figure 6, we can see that the packet drop of our proposed NSATA is 78% less than the existing ITRM protocol.

From figure 7, we can see that the resilience of our proposed NSATA is 84% less than the existing ITRM protocol.

B. Based on Speed

In our first experiment we vary the nodes speed as 5,10,15,20 and 25m/s.

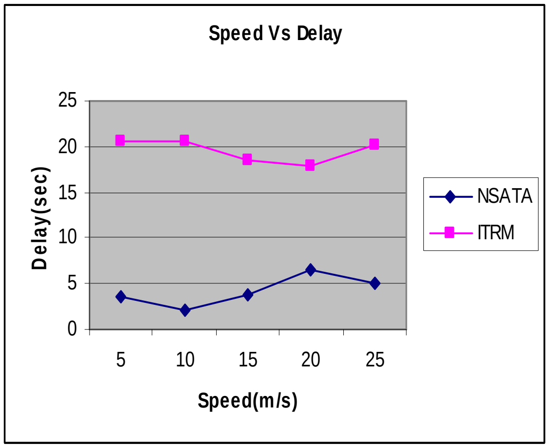

Fig 8: Speed Vs Delay

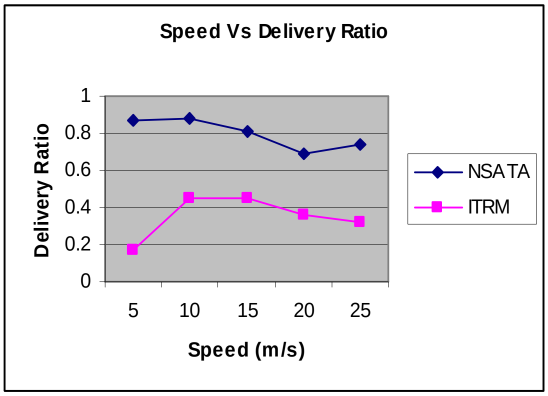

Fig 9: Speed Vs Delivery Ratio

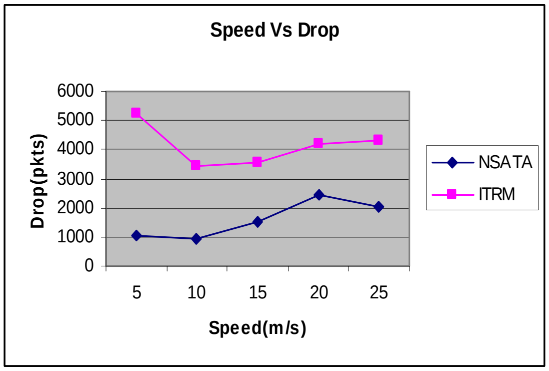

Fig 10: Speed Vs Drop

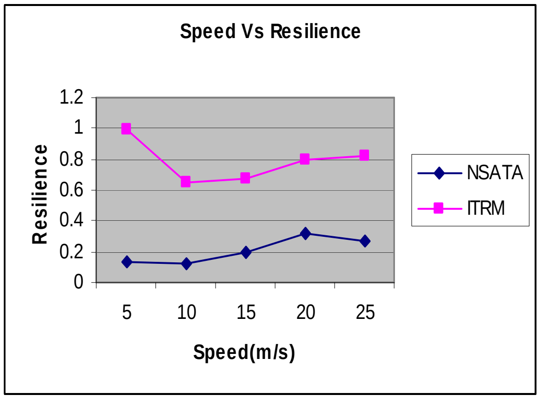

Fig 11: Speed Vs Resilience

From figure 8, we can see that the delay of our proposed NSATA is 78% less than the existing ITRM protocol.

From figure 9, we can see that the delivery ratio of our proposed NSATA is 55% higher than the existing ITRM protocol.

From figure 10, we can see that the packet drop of our proposed NSATA is 60% less than the existing ITRM protocol.

From figure 11, we can see that the resilience of our proposed NSATA is 73% less than the existing ITRM protocol.

5. CONCLUSION

In this paper, we have designed Novel security architecture for MANET for trusting and authentication. In this First phase multiple paths are determined based on AOMDV and the end-to-end packet success rate is sent as feedback to the source by the destination. It is estimated based on the packet error rate which is modeled at each network node as a random process for capturing the nondeterministic and dynamic effects of the jamming attack. In this Second phase, based on the method for trust and reputation management is then applied. In this Third phase, a standard authentication scheme for MANETs is proposed using Threshold Secret Sharing to provide security inside a network allowing only the legitimate users to utilize the network. In this algorithm multiple Certification Authority (CA) nodes are selected based on the evaluated reputation index, transmission power and mobility. Threshold cryptography is implemented in the network to less overhead and faster completion of the authentication process is achieved.

REFERENCES

[1] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE Transactions on Industrial Electronics, Vol. 60, No. 3, March 2013.

[2] Haiying Shen and Lianyu Zhao, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs", IEEE Transactions On Mobile Computing, Vol. 12, No. 6, June 2013.

[3] Dimitrios D. Vergados and Giannis Stergiou , "An authentication Scheme for adhoc networks using Threshold Secret Sharing"2007 Wireless Pers Commun 43:1767–1780 ,springer.

[4] Lung-Chung Li and Ru-Sheng Liu : "Securing Cluster-Based Ad Hoc Networks with Distributed Authorities" 2010 IEEE Vol 9.No.10.

[5] Shengrong Bu, F. Richard Yu, Xiaoping P. Liu, Peter Mason, and Helen Tang, "Distributed Combined Authentication and Intrusion Detection with Data Fusion in High-Security Mobile Ad Hoc Networks", IEEE Transactions On Vehicular Technology, Vol. 60, No. 3, March 2011.

[6] Shane Balfe, Po-Wah Yau and Kenneth G. Paterson: "A Guide to Trust in Mobile Ad Hoc Networks"2010 onlinelibrary.Wiley.com security and communication Volume 3,Issues 6.

[7] Avinash Srinivasan, Joshua Teitelbaum,Huigang Liang,Jie Wu and Mihaela Caredei: "Reputation and trust-based systems for adhoc sensor networks" In Algorithms and Protocols for Wireless Ad-Hoc and Sensor Networks, A. Boukerche (ed.), 2008 Wiley & Sons.

[8] D.Ganesh and M.Sirisha: "Reputation and Trust Evaluation in MANETs Using Eigen Trust Algorithm"2012 VSRD International Journal of CS & IT Vol. 2 (3).

[9] Swapnali sundar Sadamate and V.S.Nandedkar: "Review paper on calculation, Distribution of trust and Reputation in MANET"2013 International Journal of science and modern Engineering (IJISME) Volume 1, Issue 6.

[10] Jaydip sen: "A Distributed Trust and Reputation Framework for Mobile adhoc networks", Communications in computer science Volume, Springer.

[11] Julien Freudiger, Maxim Raya, and Jean-Pierre Hubaux : "Self-organized Anonymous Authentication in Mobile Ad Hoc Networks"2009 Social Informatics telecommunications Engineering Vol19, Springer.

[12] Erman Ayday and Faramarz Fekri, "An Iterative Algorithm for Trust Management and Adversary Detection for Delay-Tolerant Networks", IEEE Transactions on Mobile Computing, Vol.11, No. 9, September 2012.

[13] Issa Khalil and Saurabh Bagchi, "Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Countermeasure", IEEE Transactions on Mobile Computing, Vol. 10, No. 8, August 2011.

[14] Johann van der Merwe, Dawoud Dawoud and Stephen McDonald, "Trustworthy Key Management for Mobile Ad Hoc Networks", ACM Computing Surveys (CSUR), Volume 39, Issue 1, 2007

[15] Zhi Xu, Hungyuan Hsu, Xin Chen, Sencun Zhu, and Ali R. Hurson: "AK-PPM: An Authenticated Packet Attribution Scheme for Mobile Ad Hoc Networks"2012 springer Berlin Heidelberg.

[16] Patrick Tague, Sidharth Nabar, James A. Ritcey, and Radha Poovendran, "Jamming-Aware Traffic Allocation for Multiple-Path Routing Using Portfolio Selection",2011 IEEE/ACM Transactions on Networking, Vol. 19, No. 1.

[17] S. W. Roberts, “Control chart tests based on geometric moving averages,” Technometrics, vol. 42, no. 1, pp. 97–101, Feb. 2000.

[18] Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1997). Handbook of applied cryptography. CRC Press.

[19] Yi, S., & Kravets, R. (2002). Key management for heterogeneous ad-hoc wireless networks. In Proceedings of the 10th IEEE International Conference on Network Protocols, pp. 202–203.