A 50-50 PACKET TRADE MODEL IN MANET TO DETECT MISBEHAVING NODES BY ZKP AUTHENTICATION PROTOCOL

[1]S.NEELAVATHY PARI, [2]D.SRIDHARAN
[1]Assistant Professor, Department of Computer Technology
MIT Campus, Anna University, Chennai, India
[2]Associate Professor, Department of Electronics and Communication Engineering
CEG Campus, Anna University, Chennai, India
E-mail: [1]neela_pari@yahoo.com, [2]Sridhar@annauniv.edu

ABSTRACT

Mobile Ad hoc Network (MANET) is an emerging technology and hence is an active area of research. The ease of deployment and defined infrastructureless feature these networks find applications in a variety of scenarios ranging from emergency operation and disaster relief to military service and task force. Providing security in such scenarios is critical. Zero Knowledge Protocol (ZKP) help a prover convince a verifier that he /she holds some knowledge (usually secret), without leaking any information about the knowledge during verification process (zero knowledge).This paper briefly state the zero knowledge protocol to authenticate nodes in MANET and explore the game based approach for the detection of misbehaving nodes using 50-50 packet trade model, which ensures the selfish node to cooperate and detect maliciousness with low probability error. The simulation results have proved the effectiveness of the proposed Malicious Node Detection using Trade model (MNDT) with improved throughput, packet delivery ratio, and end-to-end delay as compared with existing protocols.

Keywords: *Mobile Ad hoc Networks (MANET), Zero Knowledge Protocol (ZKP), authentication, packet trade model, malicious nodes*

1. INTRODUCTION

MANET is gaining popularity and its application is increasing day by day due to its dynamic nature and ease of deployment without any base station. The mobile nodes in a MANET self-organize together in some arbitrary fashion. These networks can be applied between persons or between vehicles in areas which are depleted of fixed infrastructure. These areas could be military battlefield or some flood or earthquake affected areas. Two nodes can directly communicate with each other if they are within the radio range. If the nodes are not within the radio range they can communicate with each other using multi hop routing. The attacks in the MANET can be external or internal. An external attack cause's congestion sends false routing information or causes unavailability of services. In an internal attack the malicious node from the network gains unauthorized access and impersonates as a genuine node. It can analyze traffic between other nodes and may participate in other network activities [1].

Cryptography-based secured technologies commonly use confidentiality, authentication, integrity and nonrepudiation to provide network and information security. Authentication is the verification of the identity of the entities that communicate over the network. Without authentication, anyone in the network can forge and impersonate others. Hence cryptosystems use various techniques and mechanism to authenticate both the initiator and receivers of the data [2]. The objective of this paper is to develop a secure mechanism that protects the closed MANET against malicious behavior from outside nodes as well as insider nodes that can be used in highly confidential application such as defense systems.

The paper is organized as follows. The section 2 discusses the related work in the literature. A brief discussion on ZKP and authentication of node by ZKP is carried on in section 3. Section 4 states the game of monopoly rules followed by MNDT algorithm by 50-50 trade model in section 5. Section 6 shows the experimental results of MNDT and the performance analysis with standard protocol.

2. RELATED WORK

Wei Liu and Ming Yu [3] describe the authenticated and anonymous routing protocol by authenticating the route request packet by group signature in MANET adversarial environment. This method defends the active anonymous attack without revealing the nodes identity.

Abdullah M. Jaafar and Azman Samsudin [4] propose a new method of zero-knowledge proof of identity based on a non-expansion visual cryptography to overcome the disadvantage of complex computation in the current zero-knowledge proof of identity protocols, thus overcoming the dependence on computing devices. Since most of the security of zero-knowledge proof of identity protocols is based on complex mathematical algorithms and is required heavy computations for parties involved, the prover and the verifier [5]. A new zero-knowledge proof of identity protocol with a comparatively low and simple computation complexity and without the need for any special tools is proposed. The drawback of Visual zero knowledge proof of identity is that it will be built with only Boolean OR operations but not with any other operations.

Mahmood Khalel Ibrahem [6] explains about the Diffie–Hellman (D-H) key exchange algorithm was developed to exchange secret keys through unprotected channels. In this paper D-H algorithm has been modified into an interactive zero-knowledge proof protocol.The proposed protocol is designed to satisfy the zero knowledge proof properties and resists the known attacks. Two versions of the proposed protocol are presented - the first one was built around the basic D-H key exchange algorithm, which is vulnerable to man-in-the middle attack.The second proposed version solves the problem of the mentioned attack.First drawback is Zero-knowledge proofs are probabilistic proofs because there is some small probability (soundness error) that allows a cheating prover to convince the verifier of a false statement. Second drawback is Standard techniques used to decrease the soundness error to any arbitrarily small value, but with additional computation cost.The Third drawback is the proposed protocol fulfills the ZKP properties and protected against discrete logarithm attack and man-in-the middle attack.

Siba K Udgata [7] addresses some other special security threats and attacks in WSNs.This paper propose a scheme for detection of distributed sensor cloning attack and use of zero knowledge protocol (ZKP) for verifying the authenticity of the sender sensor nodes.The ZKP is used to ensure non transmission of crucial cryptographic information in the wireless network in order to avoid Man-In-The Middle (MITM) attack and replay attack. Thus the paper presents a detailed analysis for various scenarios and also analyzes the performance and cryptographic strength.In future, the work can be extended to detect the passive attacks and evaluate performance in real time using TinyOS and Tossim.

Sudhir Agrawal and Sanjeev Sharma [8] has attempted to present an overview of the routing protocols, the known routing attacks and the proposed countermeasures to these attacks in various works. Due to lack of a defined central authority, securitizing the routing process becomes a challenging task thereby leaving MANETs vulnerable to attacks, which results in deterioration in the performance characteristics as well as raises a serious question mark about the reliability of such networks. Although researchers have designed efficient security routing, optimistic approaches which can provide a better solution is tradeoff between security and performance.

In the previous work [9] zero knowledge protocol for authentication in MANETs based on the mathematical theory of Pythagoras has been proposed. In this paper the proof of completeness, soundness and zero knowledge is presented. Overtime, trust values of nodes may change and it is essential that nodes are continuously monitored for malicious behavior. The extension of this work using game model is presented in this paper.

3. ZERO KNOWLEDGE PROTOCOL

A zero-knowledge proof of identity protocol is a special cryptographic algorithm for identity verification. The security of most of the zero-knowledge proof of identity protocols is based on complex mathematical algorithms and requires heavy computations for both parties involved, the prover and the verifier. Thus, the two parties must depend on computing devices to perform these computations.

The purpose of ZKP protocols is to help a prover convince a verifier that he /she holds some knowledge (usually secret), without leaking any information about the knowledge during the verification process (Zero-Knowledge). The concept of ZKP was first introduced by Goldwasser et al. [10] and has since been employed in many authentication and identification protocols.

A ZKP is an interactive proof system, which is comprised of a prover and a verifier. The principle rule is that the prover demonstrates knowledge of a secret to the verifier through several interactive rounds. During the process, the prover does not reveal any sensitive information to the verifier or any other parties. Each round involves a challenge (say, a question) from the verifier and a response (say, an answer) from the prover. If the secrets are related to user identities, ZKP can be used for identification and, in this case, is called Zero-Knowledge Proof of Identity (ZKPI).

3.1 Authentication of Node by ZKP

The Secure User Groups (SUGs) is defined as the group of mobile nodes that can only make calls and receive calls from members within the group or outside the group but only on passing high security requirements [13]. These groups may be referred to as Intelligent and Secure Groups (I&SG) in the defence. A node may be a member of more than one SUG, be permitted to make calls outside of the SUG (Outgoing Access) and be permitted to receive calls from outside of the SUG (Incoming Access). The ZKP for authentication based on primitive pythagorean triples and its proof has been dealt in length by the author [9]. A Pythagorean triple is a set of positive integer a,b,c that fits the rule a2 + b2 = c2. Pythagorean triples a, b, c in which gcd (a,b,c) =1 is called the Primitive Pythagorean Triple (PPT). L, R, M is the Left, Right and Middle triples, successor of X Triplets. The Figure 1 shows the working function of the ZKP authentication protocol.

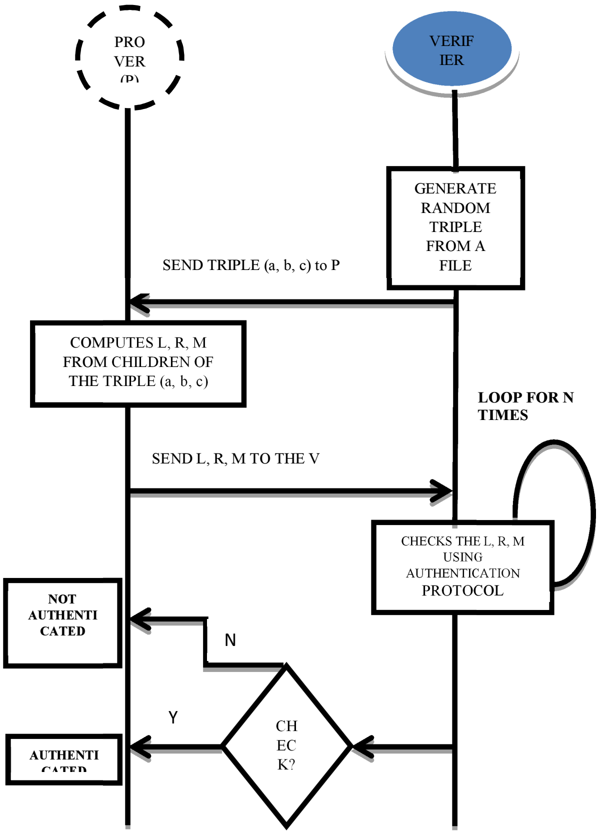
PRO
VER
(P)
VERIF
IER
GENERATE RANDOM TRIPLE FROM A FILE
SEND TRIPLE (a, b, c) to P
COMPUTES L, R, M FROM CHILDREN OF THE TRIPLE (a, b, c)
LOOP FOR N TIMES
SEND L, R, M TO THE V
CHECKS THE L, R, M USING AUTHENTICATION PROTOCOL
NOT AUTHENTI CATED
N
Y
CH EC K?
AUTHENTI CATED

Figure 1: Zkp Authentication PROTOCOL

4. GAME OF MONOPOLY

To BUY / RENT / SELL properties so profitably that one becomes the wealthiest player and eventual MONOPOLIST.

4.1 Rules of the Game

- The game can be played between two to eight players. Each player gets to select the pewter pawn.
- Every player receives about $1500 in cash.
- The sequence of players is decided by rolling two dice.
- One player can act as a banker of the game. He has to keep his and the banksmoney separate.
- The first player rolls over the two dice and moves the pewter to equal number of spaces. (Although the official Monopoly game rules state that the first player has to be the banker.)If the

player manages to roll a double dice, then he gets another chance to roll again.

- The property on which the player lands after rolling the dice, if it is not owned by anyone, that player has the option of buying the property.
- If the player lands on the property that is owned by someone else, then the owner has to collect the rent.
- If the property is mortgaged, then the rent cannot be collected.
- When a player lands on chance or community spaces, he can draw a card from the corresponding decks, and do what it says.
- When the player buys a property, he has the option of buying hotels and houses. This increases the rent of the property, and whenever another player lands on such places, the owner gets the increased rent.
- A player can only build a hotel if he has bought four houses.
- The player can buy, sell, or even trade the properties with other players.
- When the player lands on the income tax space, the player has the option of paying either $200 or 10% of his total worth to the bank. The option of paying $200 can only be exercised before calculating his total worth. Once it has been done, the player has no option but to pay 10% of his cash.
- If the player rolls the triple dice, then he has to go to jail. This is also true when the player lands on the 'Go to Jail' space. He can get out of jail either by paying $50 or rolling a double dice again.
- If a player is bankrupt and owes another player some rent, he has to give his property to other players.
- The game ends when only one player is left and all the other players are bankrupt.

5 MALICIOUS NODE DETECTION ALGORITHM

5.1. 50 -50 Packet Trade Model

The basic idea of credit-based schemes is to provide incentives for nodes to faithfully perform networking functions. In order to achieve this goal, virtual (electronic) currency or similar payment system may be set up. Nodes get paid for providing services to other nodes. When they request other nodes to help them for packet forwarding, they use the same payment system to pay for such services .Here the concept of nuggets (also called beans) is used as payments for packet forwarding. Nuggets are loaded into the packet before it is sent. The sender puts a certain number of nuggets on the data packet to be sent. Each intermediate node earns nuggets in return for forwarding the packet. Each intermediate node "buys" the packet from the previous node for some nuggets, and "sells" it to the next node for more nuggets. Thus, each intermediate node earns some nuggets for providing the forwarding service, and the overall cost of sending the packet is borne 50% by the source and 50% by the destination.

5.2. Architecture

Here we consider the cluster based approach. Clusters represent SUGs. Nodes that are part of two clusters are said to be gateway nodes. All intra group communications must go through the cluster head only and inter group communications go through the gateway nodes. The cluster head represents the Verifier (V) who authenticates all other member nodes (Provers) of the group [11], [12]. The architecture is as shown in Figure 2.

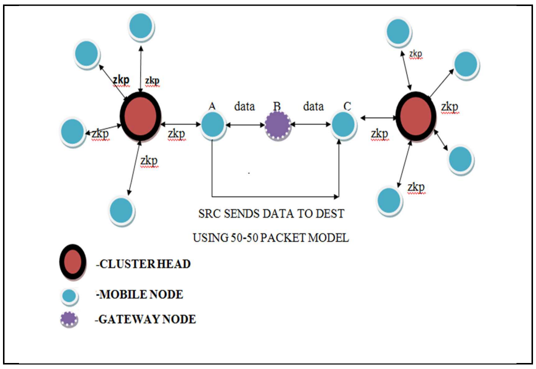

Figure 2: Architecture Diagram

5.3. Pre-Requisites

Assumptions:

Let a node B buy a packet for '*x*' beans from A and forward it to C by obtaining '*y*' beans from C. We assume forever that ' $y>=x$ '. The CH always has infinite amount of beans.

Beans: Virtual currency used in trading of packets

Data structures used:

WhiteList: List of non-malicious nodes.

BlackList: List of malicious/ selfish nodes.

GreyList: List of nodes suspected to be malicious during the operation of the algorithm.

A node may move from GreyList to BlackList / WhiteList. No node may move directly from WhiteList to BlackList or vice versa but only through the GreyList.

5.4. Algorithm

Step 1: Initial supply of virtual currency

Initially CH gives every node some number of beans based on the energy of the node as shown in Figure 3. For e.g. if energy =100 then 50 beans are given. However this is implementation dependent. More energy implies more participation in packet transfer. Hence more beans are supplied by the CH to nodes with more energy.

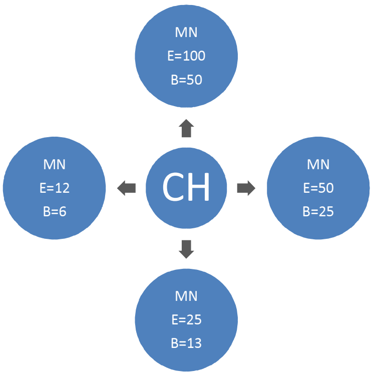

Figure 3: Initial supply of virtual currency

Step 2: Start trading of packets using 50-50 packet model

If A wants to send a packet to C, Let us assume path chosen by routing protocol is A--->B--->C. Now B gives say 20 beans to A and gets the packet. Later B sells the packet to C (usually for a higher price say 30) thereby earning a profit of 10 beans. Now A has spent nothing to send the packet but C has spent 30 to receive the packet which is unfair. So the CH takes 15 (exactly 50 % of beans spent by destination from sender of the packet) and gives it to the receiver as shown in Figure 4. (Hence the name 50-50 packet model).

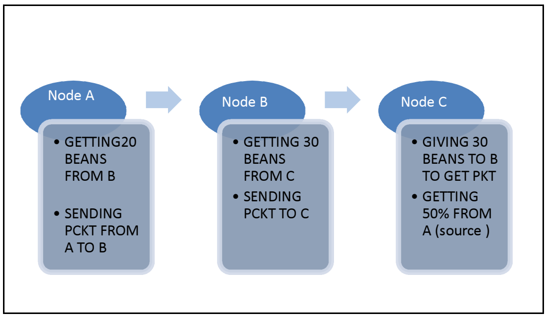
Node A
• GETTING20 BEANS FROM B
• SENDING PCKT FROM A TO B
Node B
• GETTING 30 BEANS FROM C
• SENDING PCKT TO C
Node C
• GIVING 30 BEANS TO B TO GET PKT
• GETTING 50% FROM A (source)

Figure 4: Trading of packets using 50-50 packet model

Step 3: Network Monitoring

At regular intervals the CH sends some amount of beans to all the nodes based on the energy. These beans are essential for trading. If a node does not have sufficient amount of beans then it can obtain essential amount of beans from the CH but has to repay within a particular amount of time. If it fails to do so, the node is added to the GreyList.

Let ' *x'* be the minimum number of beans received to send 1 packet, '*y*' be the minimum number of beans spent to receive a packet, '*r'* be the number of packets received and *'s'* the number of packets sent.

A non-malicious node will always want to achieve *sx – ry >= 0* for profit.

(i). *((no. of beans given to node by CH) - (sx - ry)) <= threshold*

(ii). Energy of node >= threshold

If both (i) and (ii) are satisfied then node may be malicious. Add node to GreyList M. If a node fails to deliver a packet to the next hop node then the source after waiting for a particular amount of time for the acknowledgement, it sends a request to CH to monitor the route from the source to destination. The CH monitors the route as follows.

Let there be five nodes

```
                G
                |
A----->B----->C----->D----->E
                |
                F
```

A sends a packet to E through A->B->C->D->E. Assume all packets initially have 100 beans.

After trading the packet reaches D. D has received the packet from C but has not forwarded it to E, Say at time *t1*, the trading is shown in the Table 1.

Table 1: Trading scenario

Time	A	B	C	D	E
t1	100	100	100	100	100
t2	120	110	100	70	100

Now on looking at the path from A to E since D has least beans it may be malicious. This is based strongly on the assumption that every node sells its packet to the next hop node for a greater or equal price as it spent. So add node to the GreyList.

But there be one case:

Suppose node F sent a packet intended to node G through B. Then at *t2* B may have obtained the packet from F for say 30 beans but has not yet transferred it to G. So now B has only 70 beans. This does not mean that B is malicious yet it is added to GreyList. Later at t3 when the packet is transferred to G for say 35 beans, the bean value of B becomes 105 the CH finds out that it may not be malicious. So B is reverted from the GreyList. Thus constant monitoring is essential for differentiating non-malicious and malicious nodes in the GreyList.

Step 4: Monitoring for Selfish behavior in nodes

Node whose beans are neither decreasing nor increasing for particular amount of time (based on type of application) may be suspected as selfish nodes. Then we put the node in GreyList as Suspected (*GL*).

A certain percentage of beans (20%) of *GL* are taken by CH from *GL* as penalty for being idle for a certain amount of time. Thus instead of periodically giving beans to the CH , *GL* would prefer to start trading rather than being idle. Thus every node would try to reduce its selfish behavior.

CH will monitor every node labeled *GL* in the GreyList for selfishness for certain amount of time. If *GL* continues to exhibit selfish behavior, CH will move *GL* from GreyList to BlackList. Consider in SUG if a member node wants to join in the network. To join the cluster member node Prover (P) have to prove to the cluster head who acts as Verifier (V). Here exists two chances, first possibility is the member node is honest prover and the second possibility is that it may be the dishonest prover. This proof is dealt in detail in [9].

6. PERFORMANCE EVALUATION

The algorithm for detection of malicious nodes based on the game of monopoly has been implemented using ns2 [18].The nodes are given initial supply of beans based on their current energies. During the routing for every packet sent, trading of packets is done by using control packets such as bean reply and bean response .Using the above algorithm malicious nodes are detected using the beans and selfish nodes are made to be more cooperative.The performance of the Misbehaving Node Detection using Trade Model (MNDT) protocol is evaluated using parameters Packet Delivery Ratio, Delay, throughput and routing overhead. Table 2 lists the simulation parameters and environment used.

Table 2: Simulation Parameters

Terrain	800×800 m
Transmission Range	250 m
Mobility model	Random Way-Point
Minimum speed	0 m/s
Maximum speed	100 m/s
Traffic source Type	Constant Bit Rate
Data Rate	2Mbps
Propagation channel frequency	2.4 GHz.
MAC Protocol	IEEE 802.11
Routing Protocol	AODV, MNDT, TPRP, RSRP, AASR
Packet Size	512 Bytes
Simulation Time	100 seconds
Number of nodes	10 ~50
Initial Energy	150 joules

The simulation result is carried on in three groups. Initially the MNDT performance is analyzed varying the number of cluster and malicious nodes. In the second set the MNDT result is compared with Ad hoc On- Demand Distance Vector (AODV) protocol [17]. Finally the throughput of MNDT is compared with Trusted Path Routing Protocol (TPRP), Robust Secure Routing Protocol (RSRP), and Authenticate Anonymous Secure Routing (AASR).

Group1: The Effects of Varying Cluster Size Scenario: To simulate the adversarial environment, the varying range of malicious nodes from 1 to 5 is introduced in the network and the average delay and throughput measured is shown in the Figure 5and 6.

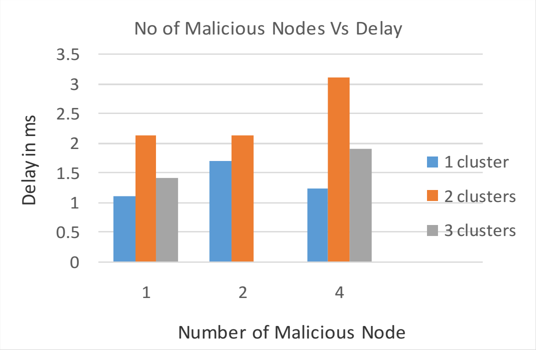

Figure 5: Delay versus no. of malicious nodes.

It is observed that the delay was in the range of 1.11ms to 1.29ms for one cluster with varying number of malicious nodes. The delay increased comparatively when two clusters involved. The simulation results in Figure 5 states that the delay is less in the three clusters when compared to two clusters. There are many parameters to be considered like the path length and how the data routed through the gateway nodes.

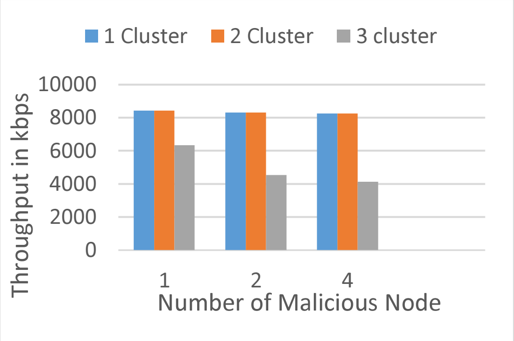

Figure 6: Throughput with varying cluster size

Group 2: The Effects of Malicious node in MNDT and AODV Protocol scenario: The network is configured with average speed of 10m/s and the number of malicious nodes is varied from 1 to 32 nodes. The results are recorded and plotted in the following Figure 7 and 8.

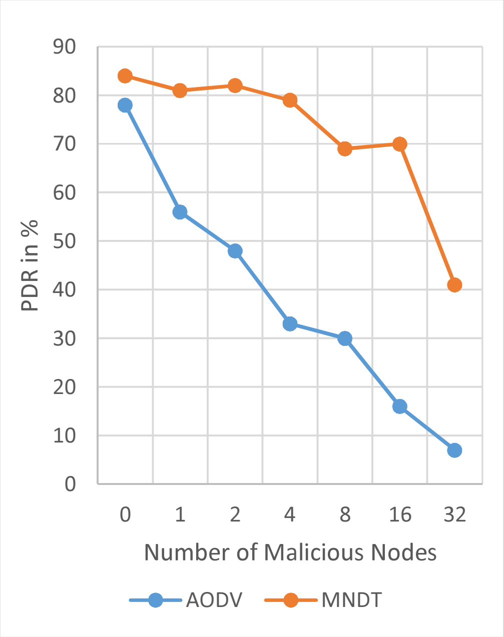

Figure 7: PDR versus number of Malicious Nodes

The effect of number of malicious nodes on packet delivery ratio for one cluster is shown in the Figure 7. The MNDT protocol has shown 84% of PDR when there is no malicious node in the network. The PDR decreased as the number of malicious node increased. When there was about 64% of malicious in the network, still the network was able to provide 41% of performance. In this method selfish node are made to cooperate as 10% of beans will be paid as penalty to CH, if the node is being idle while taking part in the route discovery.

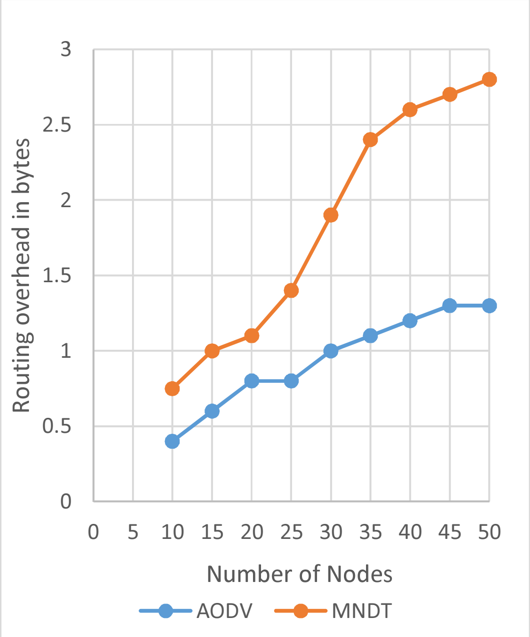

Figure 8: Routing Overhead versus Number of Nodes

The Figure 8 depicts the effect of number of nodes and routing overhead for AODV and MNDT. The routing overhead increases as the number of active mobile nodes increases in the network. This is due to the number of routing packets (data packets and control packets) between the nodes. MNDT periodically checks for authentication of nodes by ZKP algorithm. The CH verifies the node energy to supply beans of get penalty from the idle nodes. MNDT uses four different control message types: Cluster Head selects random triple from a file and sends to the node prover (P). The prover sends L, R, M calculating from the predefined matrix A, B, C [7].

Each intermediate node sends the control packet (number of beans) and receives beans for transmitting the packet. When the packet reaches the destination, the destination receives 50% of beans from the source node. Hence the amount of beans required for transmission is shared equally by the source and the destination.

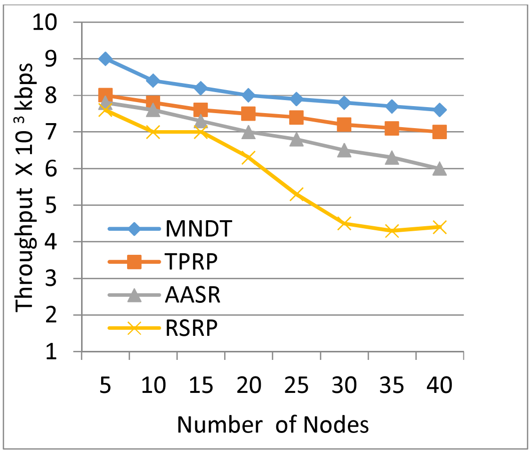

Figure 9: Comparison of MNDT with standard protocols

The Figure 9 illustrates the performance (throughput) of Trusted Path Routing Protocol (TPRP), Robust Secure Routing Protocol (RSRP), and Authenticate Anonymous Secure Routing (AASR). The TPRP method favour packet forwarding by maintaining the trust and reputation table for each node [15]. The trust is evaluated based on direct and indirect observation of nodes performance. The source node selects the most trusted path than the shortest path. The RSRP [16] is based on broadcast authentication. This scheme assumes pre distribution of key and secret key is shared among the pair of nodes before communication. In AASR each route request packet is authenticated by group signature using key-encrypted onion to record discovered route and design encrypted secret message to verify route request and route reply control messages. In MNDT only the authenticated nodes can participate in the network and the probability of malign nodes is zero. If the authenticated node (internal node) turns into dishonest node (stealthy attack) the MNDT protocol identifies this node as this protocol is based on packet trade model.

When the number of nodes increased (10% of malicious nodes), there was a decrease in throughput. TPRP, AASR and RSRP spends time in calculating trust for each packet routed and security processing in exchanging key values. MNDT achieves an average 3% of higher throughput for the simulated scenario with 10% of malicious nodes.

7. CONCLUSION

There are many reasons for implementing ZKP as well as providing higher level of security. It allows someone with no knowledge on how the protocol functions, to take advantage of concept. The system is transparent to user and it is simple and ease of implementation is definitely a value-added reason to have this application for MANET. The performance of MNDT has been analyzed by varying the number of cluster in the network. The performance is compared with AODV routing protocol.

The simulation result shows that higher throughput, packet delivery ratio, lower end-to-end delay is achieved. It has higher routing overhead than AODV due to authentication and reducing the selfish behavior, by making the node to cooperate with the network. MNDT is compared with three standard algorithms. The 50-50 trade model ensures proper transmission of packet as the entire intermediate nodes does trading the amount incurred for trading is shared by sender and the receiver. This method has prevailed over the attacks like DoS attack, Man-in-the-middle attack and eavesdropping and replay attack.

REFERENCES:

[1] Rashid Sheikh, Mahakal Singh Chandee and Durgesh Kumar Mishra, "Security Issues in MANE A Review", *IEEE Seventh International Conference on Wireless And Optical Communication Networks*, 2010, pp. 1-4.

[2] Jianmin Chen and JieWu, "A Survey on Cryptography Applied to Secure Mobile Ad Hoc Networks and Wireless Sensor Networks", *8TH International Conference, ACNS 2010, Beijing, China Proceedings*, Vol. 5, 2010, pp. 2414-2424.

[3] Wei Liu and Ming Yu, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments*", IEEE Transactions on Vehicular Technology*", Vol 10, March 2014, pp 1-9.

[4] Abdullah M, Jaafar and Azman Samsudin, "Visual Zero-Knowledge Proof of Identity Scheme: A New Approach", *IEEE Second International Conference on Computer Research and Developments*, 2010, pp. 205 – 212.

[5] UrielFeige, Amos Fiat and Adi Shamir, "Zero Knowledge Proof of Identity", In Proceedings of the 19th ACM Symposium on Theory of Computing , 1987, pp.210 -217.

[6] Mohmood Khalel Ibrahem and Tamara Alaa M Ali, "Secure Messaging System using ZKP", *International Journal of Computer Science Engineering and Technology,* November 2013, pp.388-393

[7] Siba K Udgata, AlefiahMubeen ,andSamrat L, "Wireless Sensor Network Security Model Using Zero Knowledge Protocol", *IEEE International Conference On Communications (ICC)*, 2011, pp. 1-5.

[8] Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks", *Journal Of Computing*, ISSN 2151-9617, Vol. 3, 2011, pp 66-67.

[9] S.Neelavathy Pari and D.Sridharan, "Zero Knowledge Protocol for Authentication based on Primitive Pythagorean Triples", *Jokull Journal, Vol* 64, January 2014 pp 248 -260.

[10] Shafi Goldwasser and Rafail Ostrovsky, "Invariant signature and non-interactive Zero-Knowledge Proofs and Equivalent", Advances in Cryptography, 1993, pp.22-245.

[11] Cynthia DworkMoniNaori, "Zaps and Their Applications", *IEEE Transactions On Information Theory*, Vol. 42, No. 6, 2007, pp. 283-293.

[12] Slawomir Grzonkowski, Peter M Corcoran Thomas Coughlin, "Security Analysis of Authentication Protocols for Next-Generation Mobile and CE Cloud Services",*IEEE International Conference On Consumer Electronics - Berlin (ICCE-BERLIN),*2011, pp. 83-87.

[13] Mike Burmester and Breno de Medeiros, "On the Security of Route Discovery in MANETs",*IEEE Transactions On Mobile Computing,* Vol. 8, No. 9, 2009, pp.1180-1188

[14] Slawomir Grzonkowski,Peter M Corcoran (2011), Thomas Coughlin, "Security Analysis of Authentication Protocols for Next-Generation Mobile and CE Cloud Services',*IEEE International Conference On Consumer Electronics - Berlin (ICCE-BERLIN),*2011, pp. 83-87.

[15] S. Neelavathy Pari and D.Sridharan," Design of Cross Layered Security Architecture to Mitigate Misbehaving Nodes in Self-

Defending Network" *European Journal of Scientific Research* , Vol.77 No.1 June 2012, pp.37-45.

[16] Syed Rehan Afzal, subir Biswas, Jong-bin Koh, Taqi Raza, Gunhee Lee and Dong-kyoo Kim, "RSRP: A Robust Secure Routing Protocol for Mobile Ad hoc Networks", IEEE *Communication Society* (WCNC) 2008, pp 2313-2315

[17] Charles.E. Perkins and Elizabeth.M. Royer. "Ad hoc on Demand Distance Vector (AODV) algorithm", *IEEE Workshop on Mobile Computing Systems and Applications*, 1999, pp.90–100.

[18] NS-2, the ns Manual available at http: //www. isi.edu/nsnam/ ns/doc