Trusted and Secured Clustered Protocol in MANET

Syeda Kausar Fatima
Research Scholar,
JNTUH

Syed Abdul Sattar, PhD
Prof & Dean
SAKCET

D. Srinivasa Rao, PhD
Prof. ECE Dept.
JNTUH

ABSTRACT
Mobile Ad hoc Networks (MANETs) are subject to various kinds of attacks. Deploying security mechanisms is difficult due to inherent properties of ad hoc networks, such as the high dynamics of their topology, restricted bandwidth, and limited resources in end device. With such dynamicity in connectivity and limited resources it is not possible to deploy centralized security solution. Like many distributed systems, security in ad hoc networks widely relies on the use of key management mechanisms. However, traditional key management systems are not appropriate for them. This work aims at providing a secure and distributed authentication service in ad hoc networks. A trusted and secured clustered protocol in MANET, where clusters are formed based on **highly-trusted nodes having sufficient energy is proposed. Secured communication** with public key authentication service based on trust model and network model to prevent nodes from obtaining false public keys of the others when there are malicious nodes in the network is organised. Efforts to present energy efficient, secure and trusted clustering to enhance the security assurance and significant adaptation of trustworthy communication is presented. Simulation results demonstrate that proposed routing protocols can improve the energy efficiency, packet delivery ratio and route stability.

Keywords
MANET, Trust, Key management, Cluster

1. INTRODUCTION
A mobile ad hoc network is a collection of nodes with no infrastructure while its nodes are connected with wireless links. Nodes in the network are able to sense and discover nearby nodes. They communicate with each other by forwarding packets hop by hop in the network. Also, the topology of the ad hoc network is dynamically changing and the nodes of the ad hoc network are often mobile. A major challenge in the design of the mobile ad hoc network is to protect its vulnerability from security attacks. As in many distributed systems, security in ad hoc networks is based on the use of a key management system for authentication. Specific key management systems have to be developed to suit the characteristics of mobile ad hoc networks.

Cluster-based data transmission in MANETs has been investigated by researchers to achieve the network scalability and management, which maximizes node lifetime and reduce bandwidth consumption by using local collaboration among mobile nodes [1]. Clustering schemes [2] organized the network into one hop disjoint clusters then elect the most qualified and trustworthy nodes which play the role of cluster heads. Cluster heads are responsible for monitoring all the routing activities within the cluster itself. Thus need for secure clustering solutions which are resilient to the various security problems of MANET and provide secure and reliable clustering even in the presence of malicious nodes and attackers. Some cryptography-based clustering schemes such as [3- 6] have been designed for MANETs which are able to operate in hostile environment and use PKI or symmetric encryption techniques, but they do not offer sufficient protection against insider attackers and compromised nodes.

2. BACKGROUND AND MOTIVATION
Several trust models [8–11] have been proposed for self organizing networks in distributed paradigm. Jiang and Baras [12] examined the efficiency of trust based reactive routing protocols in the presence of attacks in the networks. This method is considered first-hand information to evaluate other node's trust values to make trustworthiness. Yan et al. [13] proposed a secure AODV based routing protocol for an ad hoc network which is established a secure end-to-end route. The trust values are calculated based on direct observation which is transitive.

Pirzada and McDonald [14] enhanced the trust management by considering the confidence level of trust of each node. They have used confidence level as a weight to compute trust value. Ghosh et al. [15] developed a trust model to strengthen the security of MANETs and they dealt with the issues associated with recommendations. Their model was utilized only trusted routes for making effective communication and isolates the malicious nodes based on the evidence obtained from direct interactions and recommendations. Ghosh et al. [16] proposed a mechanism for distinguishing selfish peers from cooperative nodes that is based on local monitoring. In order to distinguish between selfish and cooperative peers, a series of well-known statistical tests are applied for obtaining features from the observed AODV actions. The objective of mechanism design [10] is to address problem of designing incentives for nodes to provide truthful information and computing optimal system wide solution for finding the optimal cost efficient leaders. Vickrey, Clarke, and Groves (VCG) model is applied for node incentives to ensure truth telling to be the dominant strategy for any node. They have proposed local election algorithms, namely, cluster-dependent leader election and cluster independent leader election which provided globally optimal election solutions with a low cost. The Nodes with the most remaining energy are elected as the cluster head. This approach makes storage overhead because the cluster head kept an extra service table and each node maintains a reputation table and neighboring nodes list.

Milan et al. proposed a scheme [17], where a game theoretic model is applied to study the impact of collisions on a hop-by-hop reputation based mechanism for regular networks with uniform random traffic. The nodes in MANETs are equipped with different resources and provide discrete services. It did not deal with irregular topologies and non-uniform routing. It also discussed the perception and interaction asymmetries that could impair cooperation between nodes. Safa et al. presented a cluster based trust aware routing protocol (CBTRP) [18] to ensure secure routing path and established the trust based environment. This mechanism is used to distinguish the trusted nodes from malicious nodes. CBTRP makes use of the weighted clustering algorithm (WCA) [19] to elect cluster heads.

The weighted degrees are taken into consideration such as battery power, number of neighbors, transmission power, and mobility of the nodes to form optimal cluster head. CBTRP has also taken security into account to form trusted clusters. It organized the network into 1-hop clusters in which every node is able to elect the most qualified and trustworthy node to be its cluster head. Cluster members forward the packets through the trusted cluster heads. Malicious nodes do not forward the packets to them. In CBTRP model, the trust value is computed based on the information that one node can gather about the other node's vital information including analyzing the received, forwarded, and overheard packets. Analyzing the node's behaviour, the node is selfish, acting like a black hole, and carrying out a modification attack, fabrication attack and latency delays. This approach provides improved connectivity in MANETs in the presence of malicious nodes and also it ensured the passage of packets through trusted routes only by behavior of each node. Once a malicious node is discovered, it is isolated from the network such that no packet is forwarded from it.

Chatterjee et al. [20] proposed a secure trusted auction oriented clustering based routing protocol (STACRP) to provide trusted structured framework for MANETs. Two auction mechanisms, namely, Procurement and Dutch, determine the forward cost of one hop. STACRP organized the network as one hop clusters and elects the trusted nodes as cluster head (CH) by using a secret voting scheme. Each node maintains information of itself and its neighboring nodes for cluster maintenance. The trust model is analyzed using Markov chain which guarantees to selfish node to revoke its status from warned status to normal status by proper forwarding of others packets. This achieved a secure reliable routing solution. STACRP detected selfish nodes and enforces cooperation between nodes to achieve better throughput and packet delivery ratio with less routing overhead

Main contribution of the proposed approach is to obtain a practicable degree of tradeoffs between trust and security. Network trust metric parameters intimacy, integrity, mobility, and reliability identified and combined to evaluate the cumulative trust to provide ground level of security for human centric application with human notions. Unlike discussed trust management systems in order to growing years wise advanced technology [2, 12, 16], efforts are put forward to combine best of existing trust management models for soft security concerns while dynamically observing the impetus behavior of a node in open and dynamic pervasive environment. Exiting models are based on one or more trust or security parameters for WSN or MANETS, while our trust metric consists of five crucial trust parameters for direct and indirect communication in pervasive environment. To reduce the overheads and dependency, clustering is used for group based communication.

3. MODEL OF THE SECURE CLUSTER BASED SCHEME

The contribution of the proposed trusted secure clustering based routing protocol, TSCP are organized in two different phases such as trust management and clustering phase. In trust management phase, the protocol evaluates the node trust level in trust table with different trust factors. The trust factors present the node trust level in different states to determine trust calculation. The cluster management phase evaluates the clustering phase based on trust values and organize secure cluster communication with secured key sharing. The below sections present the detailed description of proposed protocol.

3.1 Trust Computation

We assume that each node maintains a trust table to keep trust factors with respective of communication as per node dynamic behaviour its social and QoS trust factors. Dynamic behaviour between two communicating nodes as X and Y over time t will autonomously update when it interacts with other node on demand or expiry to save resources.

Trust calculation consists of two processes, first evaluate the communicating node table credentials about trust factors and second calculates the mean of trust value based on each parameter as per predefined threshold. Consider following trust parameters for evaluating the node information.

Intimacy ($\mathrm{Tr}_{xy}^{\mathrm{intimacy}}$ (t)): it measures the interaction experiences following the maturity model [21]. It is computed by finding the ratio of positive number of interactions between nodes x and y over the maximum number of interactions over the time period [0, t] as

$$Tr_{xy}^{intimacy}\ (t) = It_x = (\frac{Pve_x}{T_x}) \quad (1)$$

Where It_x is the interaction ratio considering only positive Interaction Pve_x over total no of Interaction T_x through node x.

Integrity: this refers to the confidence of node x that node y is truthful based on node x's direct observations toward node y. Node x calculate approximately (t) by observing a count of suspicious untruthful experiences of node y that node x has observed. If the count exceeds a system-defined threshold, node y is considered totally dishonestat time t, i.e., (t) = 0. Otherwise, (t) is computed by 1 minus the ratio of the count to the threshold. It can be measured as

$$Tr_{xy}^{intigrity}\ (t) = n \times \alpha \times S \quad (2)$$

where n is normalized interaction value, α is over time t experience and S is security level of recommending Service Interface.

Mobility: Node mobility is a significant parameter to estimate the battery life where average distance between nodes required with limited energy provided. Thus average movement can measured by two factors, first the mobility incidences of the mobile nodes in a given time (t) bounded by a battery life threshold where high mobility with limited battery life will be punished that makes it highly unaffordable to achieve cooperative and second Uncertainty measures misbehaviour of nodes during failure to stabilize themselves in competitive forces where nodes are penalized for irregular haziness. Thus the node mobility misbehaviour impact can be measured for given time t as.

$$\mathrm{Tr}_{xy}^{\mathrm{mobility}}\ (t) = ((1 - \mathrm{Mo_x}(E, D) + (1 - \mathrm{Pen_x}(t)))/2 \quad (3)$$

Where $\mathrm{Pen_x}(t)$ is the x mobile node's penalty measure for visit the similar position for t times ($0 \le \mathrm{Pen_x}(t) \le 1$), and $\mathrm{Mo_x}$ () is the node x punishment credentials with $0 \le \mathrm{Mo_x}(E, D) \le 1$.

Reliability: the reliability of nodes may be evaluated in different ways, but, in general, it may be defined as the capability of nodes to respect a service agreement. This is a particular procedure that lies behind the identity certification or the encryption process. In the remaining part of this section, the word trust is used to identify the reliability of nodes also

that may be evaluated in different ways, but, in general, it can be considered as the capability of nodes to respect a service agreement. Trust based reliability over a time t can be computed as probability of packets being lost, inserted and multiplied as

$$\mathrm{Tr}_{xy}^{\text{reliability}}\ (t) = (|S_{pkt} - R_{pkt}|)/S_{pkt} \quad (4)$$

where S_{pkt} = Total no. of packets sent by Y to X and R_{pkt} = Total no. of packets received by Y sent from X.

3.1.1 Trust Calculation

The trust calculation is conducted, particularly between two neighbor nodes in a cluster. When a node X evaluates trust on another node Y at time t. We assume five trust components as described above like intimacy, integrity, energy, selfishness and reliability. The trust value that node X evaluates towards node Y at time t, $\mathrm{Tr}_{xy}(t)$, is represented as a real number in the range of [0, 1] where 0 indicates distrust and 1 complete trust.

$$Tr_{xy}(t) = TC1 \times Tr_{xy}^{intimacy} + TC2 \times Tr_{xy}^{integrity} + TC3 \times Tr_{xy}^{mobility} + TC4 \times Tr_{xy}^{reliability} \quad (5)$$

Where $TC1, TC2, TC3,$ and $TC4$ are total costs associated with these four trust factors with equal threshold of 0.25 for each trust factor and computation of all these four factors gives as a results as $TC1 + TC2 + TC3 + TC4 = 1$. Based on the higher probobability values of $TC1, TC2, TC3,$ and $TC4$ the best trust formation value will consider for formation of node trust.

Algorithm 1: Trust Evaluation

Step1 To calculate node trust based on node interaction and analyze node X and Y data.

Step 2 Calculate trust value for all four parameters

$(\mathrm{Tr}_{xy}^{\text{intimacy}}, \mathrm{Tr}_{xy}^{\text{integrity}}, \mathrm{Tr}_{xy}^{\text{mobility}}, \mathrm{Tr}_{xy}^{\text{reliability}})$

Step 3 Identify each trust parameter with corresponding trust value as per pre-defined threshold [0.0–0.2]

Step 4 Estimate the overall trust value Tr_{xy} over a specified time t

$$Tr_{xy}(t) = TC1 \times Tr_{xy}^{intimacy} + TC2 \times Tr_{xy}^{integrity} + TC3 \times Tr_{xy}^{mobility} + TC4 \times Tr_{xy}^{reliability}$$

Step 5 Finally aggregate the trust value according to weighted cost.

3.2 Cluster Formation

Clustering is a standard energy efficient technique used in mobile networks to provide locality of communication through organizing the several nodes in different virtual groups known as clusters that saves energy and reduces network contention. Here several nodes are physically neighbouring and helps to organize the pervasive ad hoc networks hierarchically. An essential operation with clustering technique is to select cluster head shown in Fig. 1. The base station or mobile base stations are satellite based setups or machines capable of analyzing the data collected from the cluster heads and displaying a global view of actions being monitored.

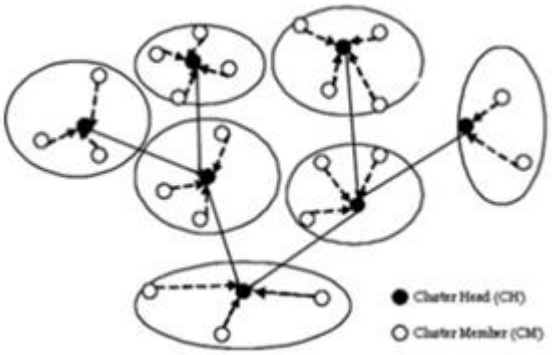

Fig 1: MANET Clustering

Inspired by Multi-objective optimization [22, 23], where multiple optimal solutions using multiple fitness functions used at same time to find optimal solution. Here fitness function is a function used to measure the optimality of a solution in evolutionary algorithm. In multi-objective optimization multiple optimal solutions using more than one objective function is used at same time.

Thus inspired by a multi-objective optimization, we use two objective functions $1(), and f2()$. The cluster head selection algorithm is based on proposed trust calculation metric as defined in Eq. (5). The algorithm initially assumes that each mobile node in the network may become a cluster head with probability 1 or 0 where nodes make autonomous decisions without any centralized control to measure the trustworthiness of the node, life time and extended security.

The fitness function in the proposed work, the fitness is evaluated based on two objective functions $f1(), and f2()$ where $f1()$ computes the trustworthiness Tr_{xy} Eq. (5) of the node, $f2()$ is used to estimate the remaining lifetime or residual energy for to elect the cluster head with a probability p which is proportional to the residual energy of the node. Thus a mobile node with higher remaining lifetime has higher possibility to become head.

Let assume NL_t is the predicted life time of the node before set up the nodes and TC_c be the time consumed to set up of the n mobile nodes as cluster, then total residual energy RE_n of all mobile nodes can be estimated as

$$RE_n = \frac{nE_{ini}(NL_t - TC_c)}{NL_t}$$

where E_{ini} is the initial energy of each node and n is the total number of nodes.

Further the probability p proportional to the residual energy can be defined to the as if NL_t number of candidates is c % of the total number of nodes with leftout energy E_l then

$$P = n \times \frac{E_l}{RE_n} \times \frac{c}{100}$$

3.2.1 Secure Cluster Communication

Assume that a MANET consist of set of clusters C where $C = \{C_1, C_2, C_3 \ldots . C_n\}$each cluster contains n number of nodes, and the public parameters in the clusters are $(H_1, H_2, H_3, P_1, P_2, \varphi, P_{pub}, n, g, h, p, \alpha, q, G_1, G_2)$. Where H_1, H_2, H_3 are cyclic groups whose orders are all q, where q

is large primer number. φ represents an isomorphic function which maps from H_2 to H_1, where α is an asymmetric function where it maps from $H_1 \times H_2 \rightarrow H_3$, non-zero generators $P_2 \in H_2^*, P_1 = \varphi(P_2) \in H_1^*$. The messages between different clusters will be forwarded by the cluster heads, due to the existence of the session keys between the cluster heads, the cluster head chooses a random number s which is belongs to Z_q, and then calculate the public key as $P_{pub} = s\,P_1$, and p and q are large primary numbers, g is a generator with q order which belongs to Z_q. Hash functions are G_1, G_2 where the messages can transmitted in the common channel. The generation of public keys across clusters and secure communication describe in next section.

3.3 Nodes Secret Shares and Key Generation

In a cluster T, the cluster head defines polynomial of degree function as

$$k-1 : f(x) = a_0 + a_1 x + a_2 x^2 + \cdots . + a_{k-1} x^{k-1} \bmod q$$

To compute the authentication key by deriving the authentication parameter as

$$\varepsilon_j = g^{a_j} \bmod p, (j = 0 \ldots . k-1)$$

This authentication key is generated at the same time to validate the authentication of node

The cluster head calculates secrete shares for the normal nodes as

$$U_i^T = f(ID_i) \bmod q$$

Then the cluster head generate the authentication parameter as a node verification where $Ver_{node} = \frac{1}{s + H_1(U_i^T || T || ID)} P_2$

The verification key is encrypted and the encrypted verification key is transferred to node

$$Enc_i\{U_i^T, \varepsilon_j, Ver_{node}\}$$

3.3.1 Key Generation

Step 1: The cluster head chooses two large primer numbers as p1 and p2 and $N = p1\ p2$

Step 2: Define a cluster key as $K = \{(N, p1, p2, c, d) : cd = 1 (\bmod \Phi(N))\}$

Step 3: Compute cluster encryption key and decryption key as follows

$$enc_k(x) = x^d \ mod\ N$$

And

$$dec_k(y) = y^c \ mod\ N$$

N and d forms a cluster public key and p1 , p2 and c forms a cluster private key

Step 4: Encrypt the message with cluster public key so that the key computation processing is reduced with the help of this and as well as reduces traffic overhead with the help of cluster key formation.

4. PERIODIC UPDATES

In this section, the key updates on different cycles to ensure the keys efficiency by updating the keys on different cycles are presented. This section describes the updates of secrete shares, node keys and cluster keys. According to the security limitations in MANET, the networks needs to get regulate key updates to ensure of security.

There are deadlines for all the circles, if this circle is over, then, the cluster will reselect the cluster head, a new service group will be formed consequently. After all the work has been done, the new cluster head will broadcast the update news to the cluster members, if the node receives the news, it needs to send its authentication parameter to the cluster head, and its qualification of update will be checked by the service group. When receive the authentication parameter from the node, the service group will judge whether $\hat{e}(H_1(U_i^T || T || ID)P_1 + P_{pub}, V_{er})$, if this statement presents true results, the service group will update the keys to the nodes.

If the authentication details failure $\hat{e}(H_1(U_i^T || T || ID)P_1 + Ppub, Ver \neq e(P1, P2)$, the node will get refused for update.

Step1 : Secret Share update : Reselection of clusterhead is based on trust value and energy level, After selection of new cluster head the new cluster head will choose a polynomial expression such as

$$S(x) = a_0 + a_1 x + a_2 x^2 + \cdots . + a_{k-1} x^{k-1} \bmod q$$

The cluster head will generate new ID's to cluster members

Step 2: Update of nodes keys : After successful node data transaction, when a node needs to send new transaction the system need to update new nodes new public key by computing the public key P_n as

$$P_n = \frac{H_1(U_i^T || T || ID)P_1 + P_{pub}}{x'}$$

Step 3: Update cluster keys: Two new large prime numbers P_1, P_2' should be chosen after the cluster head has been selected, the new cluster key will be generated as the method mentioned above, the new cluster key will be sent to all the nodes in the cluster, the broadcast will be encrypted by the new cluster key in the circle T+1.

5. SECURITY ANALYSIS

According to the MANET characteristics and security limitations there are some possibilities of potential attacks exist in the MANET. A trusted and secured clustered protocol is designed by analyzing the characteristic of the Mobile Ad Hoc Network and the potential attacks exist in the MANET, we propose a security protocol with perfect forward secrecy and backward secrecy. Even though the malicious nodes eavesdrop the traffic which is broadcasted in the network, it is impossible for them to get any useful information due to all the broadcasts are encrypted by the cluster key, only the nodes which know the key can decrypt the message. By this way, all the broadcasts can be protected well, at same time as a result of introduction of cluster key can greatly save the network resources such as bandwidth, node computational power and so on. The communications between the nodes are greatly protected as well because all of them are encrypted before transmitted by the nodes' private keys. The node without the key will never know them. In maintaining the privacy of the information, it is impossible for the node to deny the message which had been sent from it. The periodic update of keys

which is brought up in the end of protocol can resolve the problem of key leakage or loss. According to the protocol, the group network can work in a secure and more efficient manner.

6. PERFORMANCE ANALYSIS

Firstly, this section provides the computation cost and network scenario parameters for the implementation of the TSCP protocol. Then analyze the routing performance and effectiveness of the TSCP protocol in providing complete anonymity with the existing schemes through simulation results.

6.1 Simulation Setup

The proposed TSCP protocol is for MANET is implemented on ns2 simulator version 2.35. The network scenario parameters used for simulation are listed in Table II.

Table 1: Simulation Parameters

No. of Nodes	50,100,150 and 200.
Area Size	1000 X 1000
Mac	802.11
Radio Range	250m
Simulation Time	10 sec
Traffic Source	CBR
Packet Size	512
Receiving Power	0.395
Sending power	0.660
Idle Power	0.035
Initial Energy	10.0 J
Rate	5,10,15,20 and 25Kbps

In the simulation scenario an ad hoc network of size 1000m × 1000m consists of 50,100,150 and 200 mobile nodes. The mobile nodes are moving in the field according to the random waypoint model, and their average speeds range from 2 to 7 m/s. The bidirectional Constant Bit Rate (CBR) traffic is generated and the radio range of mobile node is 250m.

The proposed protocol maintains the each node trust in different trust factors, for validating each node authentication. The protocol configures trust factors to maintain node trust update parameters. During the process the TSCP protocol computes the trust based on different trust factors and determine trust evolution based on different trust parameters. The networks are organized into multiple clusters by considering each node trust value, based on the trust value and node energy level the proposed model elects a cluster head. The TSCP organizes key generation algorithms for ensuring node authentication and secured data distortion. We determine the performance by considering different key size and different network size.

6.2 Simulation Results

The performance of TSCP protocol is analyzed and the observations are made with respect to the parameters of packet delivery ratio, end to end delay, throughput and energy consumption represented in Fig 6. Fig 6 demonstrated the comparison performance of TSCP, and STACRP by varying node speeds

According to Fig. 6 (a), TSCP has the better packet delivery ratio than STACRP [20] under different mobile speed such as 5, 10, 15, 20 and 25 m/s. The packet delivery ratio of TSCP protocol is around 93.5% and for STACRP is about 92% when there is a node mobility of 2m/s. In case of STACRP, as the mobility increases the packet delivery ratio is decreased significantly about 87% to 85% when the mobile speed is 7 m/s. On the other hand, under the same scenario and mobile speed the packet delivery ratio of TSCP protocol is about 89.5%. The difference between TSCP protocol and STACRP on packet delivery ratio is less than 5%.

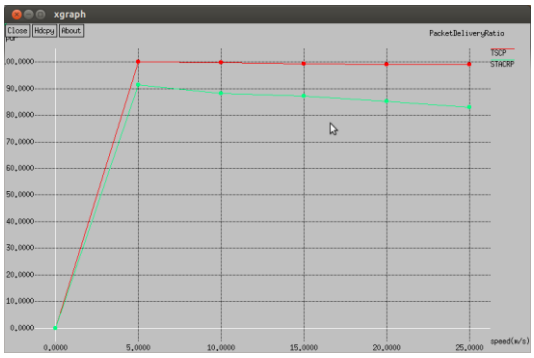

Fig 6(a) Packet Delivery Ratio vs Speed

Fig. 6 (b) shows that the comparison of TSCP, and STACRP end to end delay performance where the STACRP protocol end to end delay is increased, while mobile speed increases. TSCP performance is far better while compare to STACRP, it has less end-to-end delay.

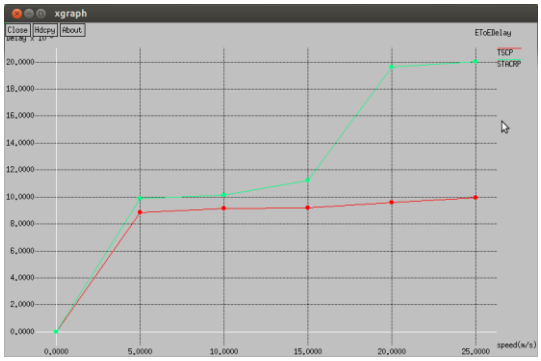

Fig 6(b) End to End delay vs Speed

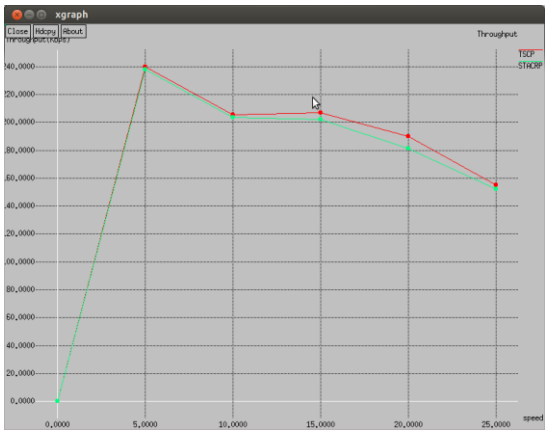

Fig 6(c) Throughput vs Speed

Fig. 6 (c), TSCP performs slightly better throughput than STACRP. The throughput of STACRP decreases as the node speed increases.

Fig. 6 (d), shows the Energy consumption, energy consumption of TSCP slightly increased while node speed increased but while compare to STACRP the energy

consumption ratio is less than STACRP. TSCP protocol energy consumption rate is almost 8 % less than STACRP.

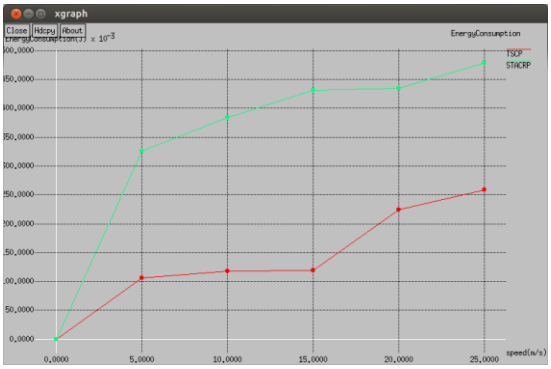

Fig 6(d) Energy Consumption vs Nodes

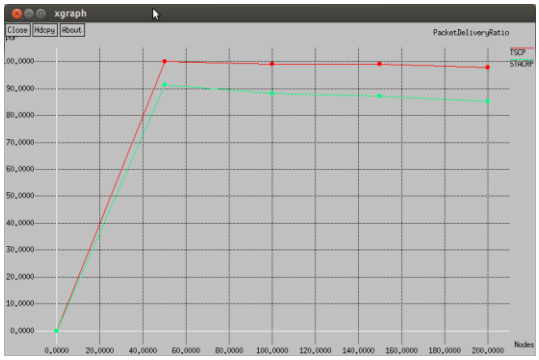

Fig 6(e) PDR vs Nodes

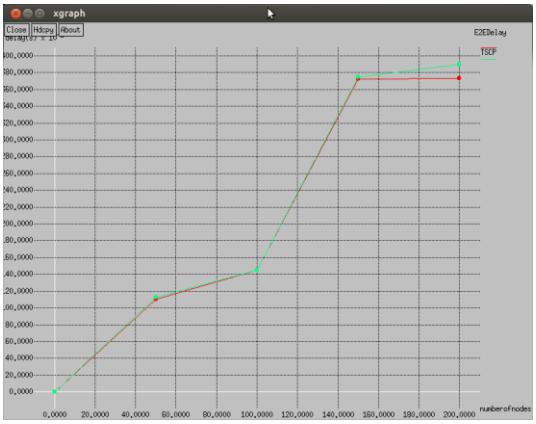

Fig 6(f) Delay vs Nodes

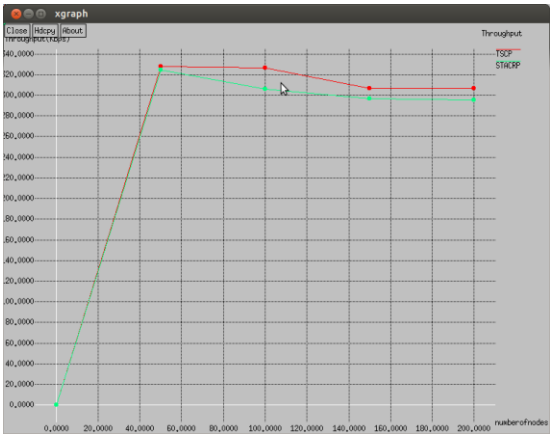

Fig 6(g) Throughput vs Nodes

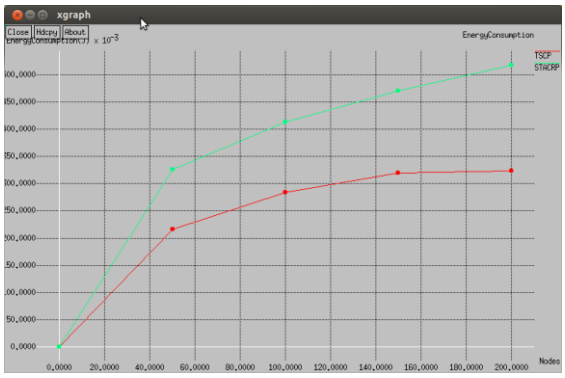

Fig 6(h) energy consumption vs Nodes

7 CONCLUSION

In this project a trusted and secured clustered protocol in MANET to organize secured and trusted communication in mobile pervasive environment is proposed. The proposed protocol organize individual node trust and reliability based on different node characteristics. Fitness functions to find out multi- dimension clustering with extended security consideration to improve energy efficient trusted clustering is formulated. A lightweight key management techniques for node authentication and secured communication with low resource computations. Based on the simulation results the proposed model perform energy efficient and robust.

8 REFERENCES

[1] A.A. Abbasi and M. Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks," Computer Comm., vol. 30, nos. 14/ 15, pp. 2826-2841, 2007.

[2] C. Tselikis, S. Mitropoulos, N. Komninos, and C. Douligeris, "Degree-based clustering algorithms for wireless Ad Hoc networks under attack," IEEE Communications Letters, vol. 16, no. 5, pp. 619–621, 2012.

[3] Y. Zeng, J. Cao, S. Guo, K. Yang and L. Xie, "SWCA: A Secure Weighted Clustering Algorithm in Wireless Ad Hoc Networks", IEEE Wireless Communications and Networking Conference WCNC, (2009).

[4] I. Nishimura, T. Nagase, Y. Takehana and Y. Yoshioka, "Secure Clustering for Building Certificate Management Nodes in Ad-Hoc Network", International Conference on Network-Based Information Systems, (2011), pp. 685-689.

[5] H. Rifà-Pous and J. Herrera-Joancomartí, "A Fair and Secure Cluster Formation Process for Ad Hoc Networks", Journal Wireless Personal Communications: An International Journal archive, vol. 56, no. 3, (2011) February.

[6] V. Sivaranjani and D. Rajalakshmi, "Secure Cluster Head Election for Intrusion Detection in MANET", Journal of Computer Applications, vol. 5, Issue EICA2012-4, (2012) February 10.

[7] M. Bechler, H. Hof, D. Kraft, F. Pahlke, and L. Wolf, "A ¨ cluster-based security architecture for Ad Hoc networks," in Proceedings of the 23rd AnnualJoint Conference of the IEEE Computer and Communications Societies (INFOCOM '04), vol. 4, pp. 2393–2403, March 2004.

[8] W. J. Adams and N. J. Davis, "Toward a decentralized trustbased access control system for dynamic collaboration," in Proceedings of the 6th Annual IEEE System, Man and Cybernetics Information Assurance Workshop (SMC '05), pp. 317–324, June 2005.

[9] A. Boukerche and Y. Ren, "A security management scheme using a novel computational reputation model for wireless and mobile Ad Hoc networks," in Proceedings of the 5th ACM International Symposium on Performance Evaluation of Wireless Ad-Hoc, Sensor, and Ubiquitous Networks (PE-WASUN '08), pp. 88–95, October 2008.

[10] R. Li, J. Li, P. Liu, and H. Chen, "An objective trust management framework for mobile Ad Hoc networks," in Proceedings of the IEEE 65th Vehicular Technology Conference (VTC '07), pp. 56– 60, April 2007.

[11] G. Theodorakopoulos and J. S. Baras, "Trust evaluation in adhoc networks," in Proceedings of the ACM Workshop on Wireless Security (WiSe '04), pp. 1–10, October 2004.

[12] T. Jiang and J. S. Baras, "Ant-based adaptive trust evidence distribution in MANET," in Proceedings of the 24th International Conference on Distributed Computing Systems Workshops, pp. 588–593, March 2004.

[13] Z. Yan, P. Zhang, and T. Virtan, "Trust evaluation based security solution in Ad Hoc networks," in Proceedings of 7th Nordic Workshop on Secure IT Systems, 2003.

[14] A. A. Pirzada and C. McDonald, "Establishing trust in pure ad-hoc networks," in Proceedings of the 27th Australasian Conference on Computer Science (ACSC '04), vol. 26, pp. 47–54, 2004.

[15] T. Ghosh, N. Pissinou, and K. Makki, "Collaborative trustbased secure routing in multihop Ad Hoc networks," in NETWORKING 2004. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications: Proceedings of the 3rd International IFIP-TC6 Networking Conference, Athens, Greece, May 9–14, 2004, vol. 3042 of Lecture Notes in Computer Science, pp. 1446–1451, 2004.

[16] T. Ghosh, N. Pissinou, and K. Makki, "Towards designing a trusted routing solution in mobile Ad Hoc networks," Mobile Networks and Applications, vol. 10, no. 6, pp. 985–995, 2005.

[17] F. Milan, J. J. Jaramillo, and R. Srikant, "Achieving cooperation in multihop wireless networks of selfish nodes," in Proceedings of the Workshop on Game Theory for Communications and Networks (GameNets '06), October 2006.

[18] H. Safa, H. Artail, and D. Tabet, "A cluster-based trust-aware routing protocol for mobile Ad Hoc networks," Wireless Networks, vol. 16, no. 4, pp. 969–984, 2010.

[19] M. Chatterjee, S. K. Das, and D. Turgut, "WCA: a weighted clusrering algorithm for mobile Ad Hoc networks," Journal of Cluster Computing, vol. 5, no. 2, pp. 193–204, 2002.

[20] P. Chatterjee, I. Sengupta, and S. K. Ghosh, "STACRP: a secure trusted auction oriented clustering based routing protocol for MANET," Cluster Computing, vol. 15, pp. 303–320, 2012.

[21] Velloso PB et al (2010) Trust management in mobile ad hoc networks using a scalable maturity-based model. In: IEEE Trans. Netw. Service Management, vol. 7, no. 3, pp 172–185

[22] Ali H, Shahzad W, Khan FA (2012) Energy-efficient clustering in mobile ad-hoc networks using multi-objective particle swarm optimization. Applied Soft Computing 1913–1928

[23] Marmol FG, Perez GM (2010) Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems. Compute Stand Interfaces 32:185–196