Efficient Node Cooperation and Security in MANET using Closeness Technique

Sathiyakumar C.[#1], K.Duraiswamy K.[#2]

[#]Department of Computer Science and Engineering
[#]K S Rangasamy College of Technology, Tiruchengode – 637 215, TamilNadu, India
[1]csathiyakumar@yahoo.com
[2]drkduraiswamy@yahoo.com

Abstract— By description, a mobile ad hoc network does not stay on any permanent infrastructure; in its place, all networking utilities (e.g., routing, mobility management, etc.) are accessed by the nodes themselves in a self-organizing manner. On the other hand, it is rigid to support cooperativeness among the nodes for their own restricted resources that require to be conserved. These scrupulous nodes which are also termed as selfish nodes decline to help other nodes in forwarding packets owing to the anxiety of having resource. Several researches design a new method that aims at attaining confidentiality of the location for an efficient communication. Thus, privacy appears from the mobile network and users gain control over the disclosure of their locations. In this work, we propose closeness mechanism accepted from the assumption of small-world event or also termed as degrees of separation to persuade cooperativeness among nodes in a trusted node's community. This paper also provides some general idea on how to develop security on the trusted MANET community by adapting security features of trust. The simulation of the proposed Efficient Node Cooperation and Security [ENCS] in MANET work is done for varying topology, node size, attack type and intensity with different pause time settings and the performance evaluations are carried over in terms of node cooperativeness, clustering efficiency, communication overhead and compared with an existing secured key model.

Keyword- MANET, Node Cooperation, Closeness Technique, Clustering, Self-Organization, Security

I. INTRODUCTION

A MANET comprises of self-directed mobile nodes that are liberated to roam subjectively with no central controller for instance router to establish the communication paths. Each node in the ad hoc network has to rely on each other so as to promote packets. This sort of MANET needs mobile nodes to contain good collaboration with each other to make certain that the commenced data communication process is success. On the other hand, it is not simple to support cooperation as there are existing nodes with selfish behaviour in the network. The selfish behaviours are forced by nodes plan to protect their own partial resources for instance battery energy, time and bandwidth. These nodes are very calculating as they use other nodes possessions for their broadcasts but hesitate to split their resources to assist other nodes processes. This phenomenon is usual because there is no middle controller or essential authority in MANET.

In a wireless network, a communication range of node will frequently not face the whole network, so end-to-end transmission might require routing information during some nodes. So, ad hoc networks are termed as multi-hop networks, where a bound is a straight link among two nodes. In an ad-hoc network, nodes are referred to as routers or terminals. Since ad-hoc network is an environment without infrastructure, the co-operation among the routers is worst. Since they are independent of each other, the problem might arise in the routing framework. The nodes can also be misbehaved. These types of nodes are referred to as selfish nodes, when selfish nodes in the network increases, then lifespan of the network will automatically decrease. The main solution to address these problems is secure routing.

Even though it is the node's precise to remain its resources at fine performance for its individual data communication operation, where that type of activities will carry no good to the successful of MANET operation as in order for a particular node to drive or accept packets, the assistance of every connecting node is very vital. Assume if all nodes in a distinct MANET environment perform selfishly, the outcome of such problem will guide to zero throughput. In MANET environments which rely seriously on nodes contribution, the reality of selfish nodes would involve the triumphant of a packet communication. Since the trouble is processed by the authoritative internal nodes, even with the consumption of the best cryptographic method will not resolve the problem. Thus, there is a requirement to propose a resolution that could promote the cooperation among nodes.

MANETs are typically self-organized networks and transitional nodes should transmit the continuous communication. To attain this, each node relies on its neighbor to promote the packet to the intention. In fact, most of preceding revises on MANETs has absolutely unspecified that nodes are supportive. As such, the concern of node cooperation becomes very imperative in MANETs. Nevertheless, cooperation may be harder to implement in MANETs than in communications based networks owing to numerous reasons. At initial stage, nodes can subjectively connect or depart the network. Second, recognition of naughtiness and consequent separation of a misbehaved node has to effort in a dispersed method owing to lack of central control. At last, user precise requirements or approach should not be overlooked. Some users observe their power resource as being restricted by battery life, and consequently they may not believe disposed to transmit track for other users. As such, user's performance will blow the system performance determined by his relevance needs or substantial constraints. In this paper, we present a technique to diminish the trouble of containing selfish nodes in MANET known as closeness mechanism that is agreed from the premise of event to promote cooperativeness among nodes in a trusted environment.

II. Related Researches: A review

Mobile Ad hoc Networks (MANETs) are renowned from further communication networks by several features. First, portable nodes in MANETs may progress liberally in the nonexistence of a permanent infrastructure. Consequently, persistent alteration in routes may ensue owing to changeable topology changes and link disconnections. Second, nodes in MANETs have restricted resources for example energy [11], bandwidth, and computational power. At last, MANETs have no faith central ability. To tackle this problem, in [1] a reputation-based system offered for DTNs to diminish the destruction fetched by selfishness. A procedure of collection ahead and a method of activities recording are offered for the discovery of misbehaving.

Intrusion detection system (IDS) acts as a dominant role in the second resistance procession of computer networks. In [2], a new anomaly detection system, called RADAR is used to identify uncharacteristic mesh nodes in WMNs. Firstly, we initiate a common concept of reputation to distinguish and enumerate the mesh node's behavior/status in terms of fine-grained presentation metrics. Current years, researchers have planned several positioning algorithms for wireless sensor networks [9]. Author in [3] proposed a Reputation-based Revising Scheme (RRS) to access the unrefined localization information before pertaining any of the positioning algorithms.

In multi-hop networks for instance mobile ad hoc networks (MANETs), a node can behave badly by falling others packets to accumulate battery life. This self-centeredness or misbehavior can interrupt the entire network functionality. To progress this, reputation based schemes are utilized for preventing white wash attacks [4]. A belief-based packet forwarding framework [5] is planned to acquire cooperation-enforcement methods exclusively supported on each node’s possess past actions and its personal defective examination of other nodes information. Author in [6] presented a method for a secure communication utilizing group key management protocol. It used ID supported confirmation key for a safe communication over ad-hoc network. An encryption technique [7] is utilized for a safe key substitute over the nodes in the network.

Cooperation enforcement [8] in independent mobile ad hoc networks under sound and defective examination and revise the essential packet-forwarding function using the recurring game models with defective information based on node cooperation [10]. The safe communication is completed based on node cooperativeness in this work by clustering according to it.

III.Proposed Efficient Node Cooperation And Security In Manet Using Closeness Technique

The proposed work is efficiently designed for enhancing cooperatives of the nodes and secure communication over MANET by adapting the closeness technique. The proposed efficient node cooperation and security using closeness technique in MANET [ECNS] comprises of three operations. The first process is evaluating the cooperativeness range of the nodes in the network. The second process is attaining the process of node cooperativeness in the network. The third process is to enhance the security of the nodes in the network. The architecture diagram of the proposed Efficient Node Cooperation and Security using Closeness Technique [ECNS] in MANET is shown in Fig. 1.

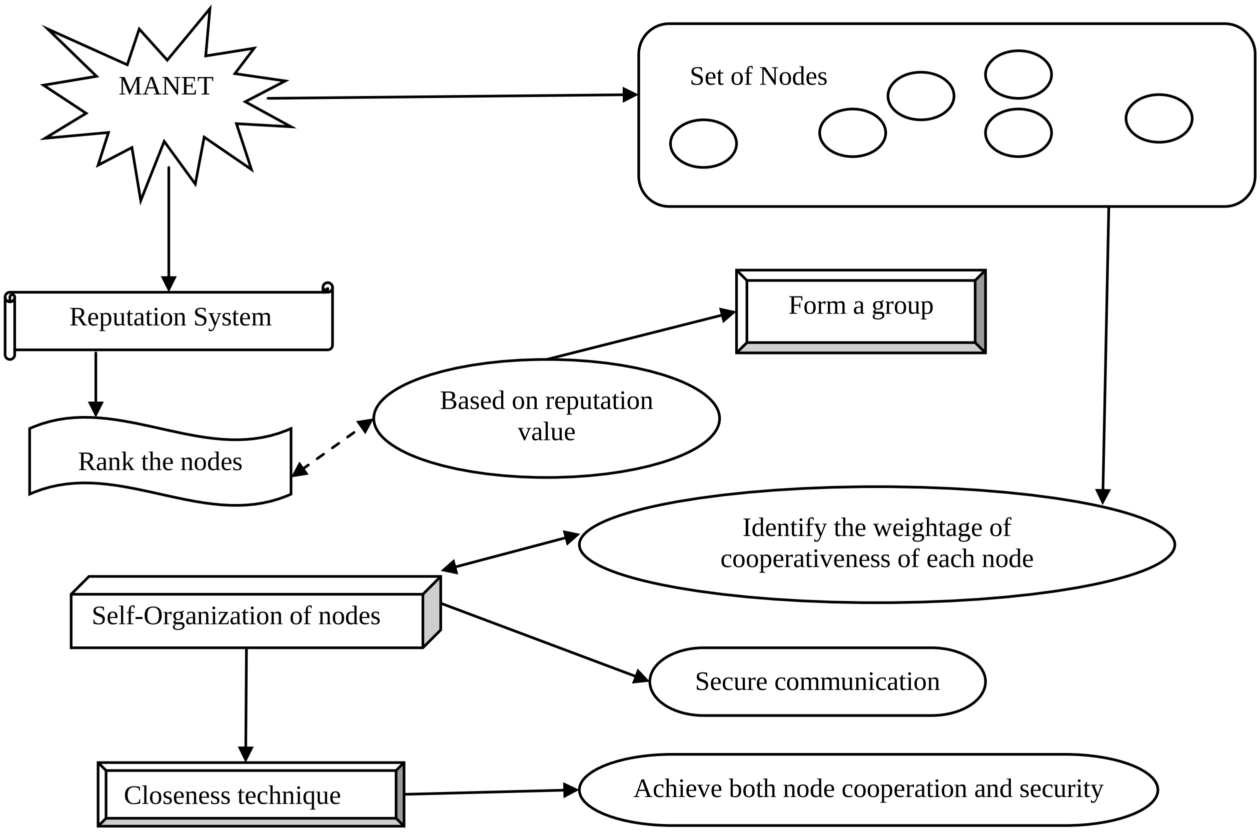
MANET
Set of Nodes
Reputation System
Form a group
Based on reputation value
Rank the nodes
Identify the weightage of cooperativeness of each node
Self-Organization of nodes
Secure communication
Closeness technique
Achieve both node cooperation and security

Fig.1. Architecture diagram of the proposed ECNS

The first process is to evaluate the cooperativeness of each node in the MANET. The evaluation of cooperativeness is done based on the behaviour and activities of the node done while the communication is taking place between the nodes. The monitoring of the behaviour of nodes is carried out and based on that the cooperativeness of the nodes is assumed. The weightage of the cooperativeness of each node is computed based on the spatial events occurred at different aspects of communication takes place. The second process is to attain the cooperatives of the nodes in the network. The third process describes about closeness technique that are able to motivate more cooperation among nodes in a MANET environment. This closeness technique is adopted from the theory of small-world phenomenon (i.e. six degrees of separation) initiated. The process of recommending trust continues until each person reaches the maximum level of the sixth degrees of friends.

From Fig. 1, it is being observed that a clustering process is presented based on reputation and ranking system in an ad-hoc network. The reputation system is enabled to allow nodes to construct informed choices regarding which nodes to assist with or prohibit from the network. To enhance the cooperativeness of the nodes, self organization of nodes is done amicably. For secure communication, closeness technique is presented to improve the security and cooperation of nodes in the network.

The expansion number of nodes is high since the ECNS mechanism processes a unidirectional trust association as an alternative of bidirectional association. A unidirectional association reveals that a distinct node could merely trust any node that it would similar to the situation of containing the entrusted nodes in the network. For instance, node A can authenticate node B in a unidirectional method devoid of containing node B’s approval. In unidirectional idea, this is measured as one preliminary trust association where as for bidirectional thought; node B must authenticates node A in return, only then one primary trust association is measured and created. The described notions can be further processed through the following Fig. 2.

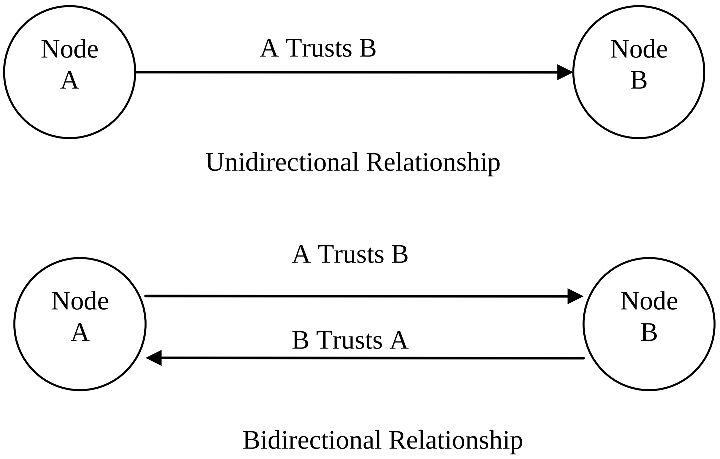

Fig. 2. Unidirectional vs. bidirectional relationship

As depicted in Fig. 2, in a unidirectional association, node B does not contain to trust node A in return to generate a trusted association. Trusted relationship among the nodes is measured since it is node A's right to authenticate either node it needs devoid of having to be trusted in return. In contrast, a bidirectional association needs both nodes A and B to authenticate each other so as to generate one trusted connection.

The idea of the proposed ENCS mechanism is the recommendation of nodes around the network about the trusted value ranges applied in MANET to increase the nodes cooperativeness of a trusted society. In security characteristic, even though this work does not affect any vital authority, the security is conserved in such a way that any two nodes are desired to contain a trusted value range before they could launch a trust association with each other. This situation comes with the statement that all trusted nodes will not contain any disobedient property at all since all involving nodes contain 100 percent reliability with each other.

A. Achieving cooperation among nodes

Cooperation among nodes in MANET is inflexible to be completed owing to the existence of self-centered nodes that do not desire to place their restricted resources (i.e. battery power, CPU and bandwidth) at risks if they vigorously concerned themselves in a packet transmission operation. For instance, a selfish node can merely crash packets that are anticipated to be thrower to other nodes as by serving forwarding those packets will disgrace its resource. This occurrence is obligatory since each node has its individual right to do so as there is no essential organizer in MANET environment to inform each node about the process of cooperation. Consequently, network operations might be paralyzed as MANET relies deeply on intermediary nodes to promote packets till complete. Nevertheless, the cooperation between nodes in MANET can be confident with the utilization of appropriate mechanism.

In this paper, we proposed a closeness technique from a small-world event concept to diminish the selfish nodes trouble. The closeness technique is processed by generating common trust between nodes before they come in a network. The common trust among nodes is fashioned by enclosing physical associations in advance which are recognized along with the relationships prepared by a particular mobile node's in the network. They have presented a mobility model depends on the association of mobile devices approved by humans. In this work, they represented the behaviour of the nodes in the network by moving in groups that present a structure of relationships. Therefore, they are capable to forecast the association pattern of nodes based on the decisions carried out by the trust values.

The same notion can be processed in this closeness mechanism whereby the construction of relationships among nodes is done based on the communications made by the users who institute common trust with each other. All the nodes' relationships uniqueness will then be processed by individual nodes to create initial trust. Nodes that have been surrounded in the proposed mechanism are extremely cooperative with each other owing to the primary trust element that has been formed in advance.

By adapting this proposed ENCS mechanism, nodes are permitted to promote packets only amongst trusted nodes in the group. As for that, nodes will not be able to assist other unidentified nodes that are not in the nodes trusted list as they are surrounded in the proposed ENCS mechanism policy. If these nodes will be punished for being selfish owing to the opposition to cooperate with other nodes which are not in the similar group of nodes, but owing to they are appreciative to pursue the rules of the group of nodes they are belong to, they will not be tagged as behave badly and therefore will not be punished. The careful forwarding activities (i.e. transmit packets only among nodes) are not only capable to avoid them from being punished but also set aside nodes' resources.

B. Enhancing Security over MANET

The closeness mechanism though afforded a secure proposal for nodes to transmit with the organization of primary trust, still facing some security threats particularly in managing compromised nodes. It is feasible for the neighbouring nodes in the trusted list to be cooperated as there has many new security attacks. In this paper, we proposed a security method by adapting features on every node to symbolize all node's in the network with the evidence properties in the reliant nodes' relationships organization process to generate a trusted MANET community. To accomplish that, we include a set of proportional studies on numerous features that have been utilized in previous works.

The security features can be categorized into two major categories:

- Performance metrics evaluation
- Quantitative trust value

In performance metrics evaluation group, the effectiveness of chosen features utilized are accessed by employing definite metrics such as route detection time, routing traffic, routing overhead and number of data packets distributed. When a source node needs to promote packet to its destination, it will request its neighbouring nodes to propose their feature's attribute number for inspection. If the neighbouring nodes handle to present an attribute number that accomplish the source node's constraint, the attribute number will be implanted in the packet format and the node is decided to promote the packet to other neighbouring nodes earlier than attaining the vital destination. The effectiveness of packet forwarding process based on selected features will be measured based on how secure the packet has been transmitted from the source to destination in a less interval of time.

C. Algorithmic Flow of ENCS mechanism

Efficient Node Cooperation and Security [ENCS] in MANET work is done for varying topology, node size, attack type and intensity with different pause time settings. The ENCS mechanism algorithmic steps are shown below

```
Start
Input      : Nodes, N1, N2, N3…Nn, Threshold Value t, Reputation Table RT
Output     : Secure Node Cooperation in MANET
Identify best t (Nn) node in MANET
For each packet data,
        Check selfish nodes from Nn nodes
// Reputation System
For Each Nn
        Assign a rank R (Nn) based on RT (Nn)
        Group the Nodes Nn based on t (Nn), R
        Choose the cluster head CHi
End For
//Closeness Mechanism
For Each Identify weight Wi
        Cooperative node Formation Ci
End For
For Inspection
        Utilize feature's attribute number ANi
For Validation
        Security Feature Selection (FS)
Form a secure channel
End
```

The above algorithm describes the reputation mechanism on the nodes N1, N2, N3…Nn in MANET with threshold value't'. The reputation system assigns the rank to the nodes based on most visited node (i.e) the cooperation provided nodes. The selfish nodes are removed as on the checking process performed in the system.

The similar numbers obtained in the ranking are grouped together in MANET. The grouped nodes based on rank are chosen as a cluster head CHi.

The closeness mechanism in mobile ad-hoc network forms a cooperative nodes Ci by removing the selfish behavior nodes. The set of nodes N1, N2…. Nn identify the weight age for the cooperativeness of node formation. The inspections are performed on packet flow based on feature attribute number and validated by selecting the particular features to form a secure channel. The closeness mechanism developed an effective cooperativeness and secure channel in mobile ad-hoc network.

IV. PERFORMANCE EVALUATION

The proposed node cooperativeness estimation and security using closeness technique is efficiently done through evaluating the cooperative rater. To estimate the performance of the proposed efficient node cooperation and security in MANET [ENCS], we run simulations on a Linux machine, having a P4-3.4GHz processor with 2GB of memory. We implement the proposed efficient node cooperation and security in MANET [ENCS] into an NS-2 environment. The simulation area extents 900x900m^2, in which nodes can move from a random starting point to a random destination, with speeds of 3, 6, 9 m/s and a pause time of 3-5 seconds. At first, the nodes cooperativeness is first identified based on the behavior and activities of the nodes in the network environment using closeness technique, after evaluating the cooperativeness value, the nodes are reorganized in a same way. Then the node clustering is done based on the directional trust range values of the neighboring nodes. Since the node clustering is performed based on weightage of cooperativeness scheme, the clustering process will be an efficient one. Then the communication among the nodes is also being good compared to an existing secured key model framework. The performance of the proposed efficient node cooperation and security in MANET [ENCS] is measured in terms of

- Node cooperativeness,
- Packet transmission time,
- Security level

V. RESULTS AND DISCUSSION

From this work, we have seen that how a secure communication is done based on the closeness technique for node cooperativeness range. Compared to an existing secured key model which runs under reputation and ranking model leads to a loss of packet at some situation, the proposed efficient node cooperation and security in MANET [ENCS] outperforms well even when the number of malicious nodes are high. The table and graph below describes the performance of the proposed efficient node cooperation and security in MANET [ENCS].

TABLE I.
Number of Nodes vs. Node Cooperativeness

Number of nodes	Node cooperativeness (%)		
	Proposed ENCS	Existing HANCC	Existing secured key model
20	56	45	20
40	69	56	35
60	78	67	48
80	84	73	57
100	92	80	70

The table (Table I) describes the cooperativeness of the nodes after applying the appropriate method. The results of the proposed efficient node cooperation and security in MANET [ENCS] are compared with an existing work[12] like HANCC [Hybrid Approach for Node Cooperation based Clustering] and secured key model.

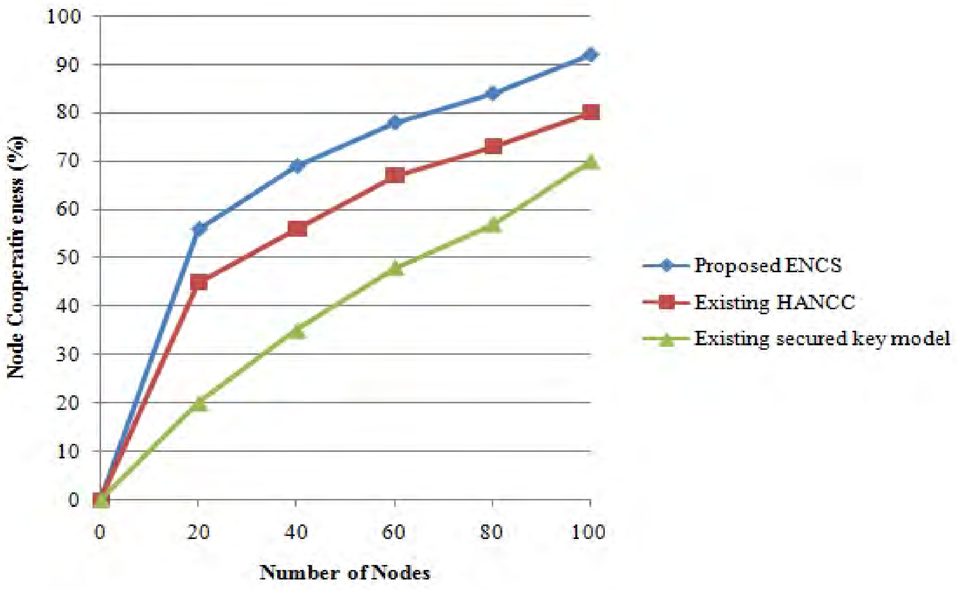

Fig. 3. Number of nodes vs. node cooperativeness

Fig. 3 describes the cooperativeness range of the nodes in the network when number of nodes increases. In the proposed ENCS, the node cooperativeness range is detected by adapting the closeness technique based on identifying the behavior and activation of the neighboring nodes. Since the cooperation of the nodes is easily detected, the proposed ENCS supports a secure communication to transmit a packet from source to destination. The node cooperativeness is measured in terms of cooperativeness range (%). Compared to an existing works like HANCC and secured key model which has been concerned only for the secure communication, if more number of node enters into the network, the existing works like HANCC and secured key model are abandoned, the efficient node cooperation and security in MANET [ENCS] outperforms well and the variance is 40-50% high in the proposed ENCS.

The table (Table II) describes the packet transmission time required to transmit the packets from source to destination. The results of the proposed efficient node cooperation and security in MANET [ENCS] are compared with an existing works like HANCC [Hybrid Approach for Node Cooperation based Clustering] and secured key model.

TABLE II.

Number of Packets vs. Packet Transmission Time

Number of packets	Packet transmission time (seconds)		
	Proposed ENCS	Existing HANCC	Existing secured key model
20	10	20	25
40	18	33	36
60	25	48	49
80	32	59	62
100	40	68	75

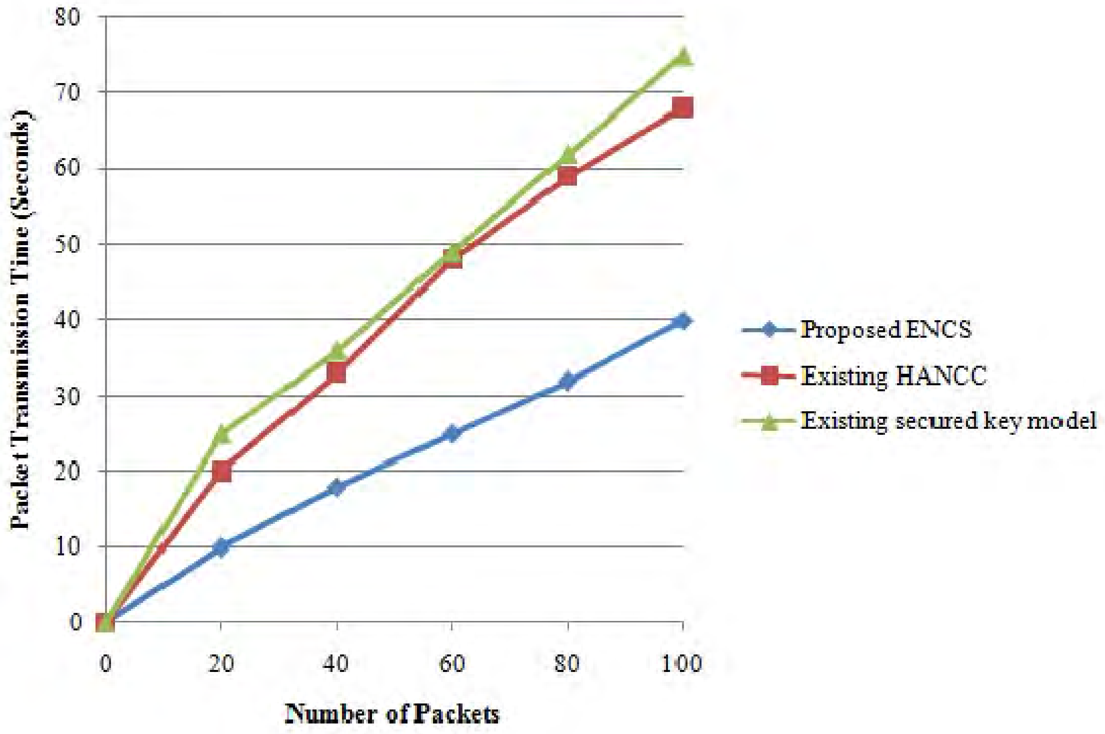

Fig. 4. Number of packets vs. packet transmission time

Fig. 4 describes the packet transmission time required to transmit the packets from source to destination. The packet transmission time is measured based on the time required to process the incoming packets from source to destination. Compared to the existing works like HANCC and secured key model, the proposed ENCS consumes less time to transmit the packet. Since the proposed ENCS presented closeness technique, the trust value of the neighboring nodes are estimated. Based on the trust values, the packets have been passed to the nearest nodes in the network. Even when the number of packets to be sent increases, the consumption of transmission time in the proposed ENCS is less and the variance is 40-50% less in the proposed ENCS.

TABLE III.
Number of Nodes vs. Security

Number of nodes	**Security (%)**		
	Proposed ENCS	**Existing HANCC**	**Existing secured key model**
50	56	40	31
100	68	48	39
150	75	56	46
200	83	64	54
250	90	73	63

The table (Table III) describes the security level of the nodes in the network environment. The results of the proposed efficient node cooperation and security in MANET [ENCS] are compared with an existing works[12] HANCC [Hybrid Approach for Node Cooperation based Clustering] and secured key model.

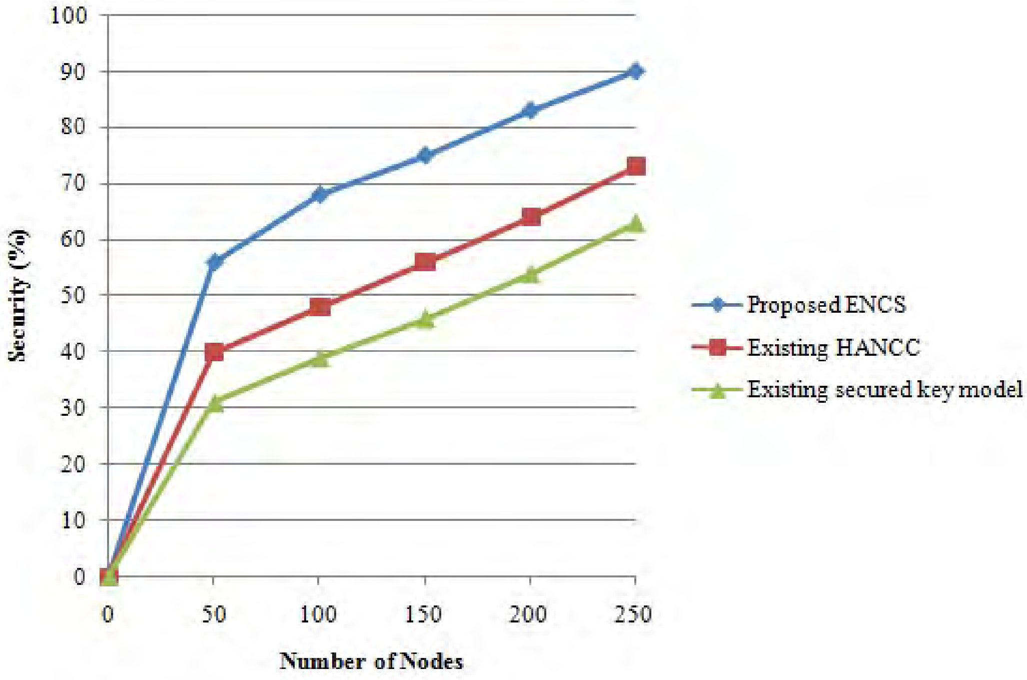

Fig. 5. Number of nodes vs. security level

Fig. 5 describes the security level of the nodes in the network environment. Since the proposed ENCS supports the security by estimating the neighboring node trust values. Based on the trust values, the level of security has been identified. Compared to the existing works like HANCC and secured key model, the proposed ENCS has high level of security and the variance is 60-70% high in the proposed ENCS. At last, it is being observed that the proposed efficient node cooperation and security in MANET [ENCS] efficiently provide a communication framework among the nodes in the network in a secure manner by evaluating the nodes cooperativeness range.

VI. Conclusion

In this paper, we have presented a ENCS mechanism to overcome the setback of selfish nodes in MANET by creating initial authentication among nodes that could improve cooperativeness since they are surrounded in MANET. This ENCS mechanism is also capable to progress security by avoiding the misbehavior nodes from replacing the security associations with unidentified nodes.

Security associations are only replaced with nodes in trusted community. So as to improve security inside the group of trusted nodes itself, we have presented the realization of features in every nodes. The selections of security features are done based on the validation that they have been commonly used in the specified network. Experimental results showed that the proposed ENCS mechanism outperforms well in terms of packet transmission and security level in the range of 70-80% high compared to the existing works like HANCC and secured key model.

References

[1] Xi Zhang, Xiaofei Wang, Anna Liu, Quan Zhang and Chaojing Tang, “Reputation-based scheme for delay tolerant networks”, International Conference on Computer Science and Network Technology, Harbin, 24-26 Dec. 2011, Vol. 2, pp. 974 – 978.

[2] Zonghua Zhang, Nait-Abdesselam, Pin-Han Ho and Xiaodong Lin, “RADAR: A ReputAtion-Based Scheme for Detecting Anomalous Nodes in WiReless Mesh Networks”, IEEE Conference on Wireless Communications and Networking, Las Vegas, 31 Mar. 2008 - 3 Apr. 2008, pp. 2621 - 2626.

[3] Xueyong Xu, Haiqing Jiang, Liusheng Huang and Hongli Xu , “A Reputation-Based Revising Scheme for Localization in Wireless Sensor Networks”, IEEE Wireless Communications and Networking Conference, Sydney, NSW, 18-21 Apr. 2010, pp. 1 – 6.

[4] S. Abbas, M. Merabti, D. Llewellyn-Jones, “Deterring whitewashing attacks in reputation based schemes for mobile ad hoc networks”, IFIP Wireless Days (WD), Venice, 20-22 Oct. 2010, pp. 1-6.

[5] Zhu Ji, Wei Yu and K.J.R Liu, “Belief-based packet forwarding in self-organized mobile ad hoc networks with noise and imperfect observation”, IEEE Conference on Wireless Communications and Networking, Las Vegas, NV, 3-6 Apr. 2006, Vol.1, pp. 343 – 348.

[6] Lung-Chung Li and Ru-Sheng Liu, “Securing Cluster-Based Ad Hoc Networks with Distributed Authorities”, IEEE Transactions on Wireless Communications, Vol. 9, No. 10, pp. 3072 – 3081.

[7] S. Sumathy and B. Upendra Kumar, “Secure key exchange and encryption mechanism for group communication in wireless ad-hoc network”, International journal on applications of graph theory in wireless ad hoc networks and sensor networks, Vol. 2, No. 1, pp. 9-16.

[8] Z. Ji, W. Yu and K. J. R. Liu, “Cooperation enforcement in autonomous mobile ad hoc networks under noisy and imperfect observations”, IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, Reston, VA, 28-28 Sept. 2006, Vol. 2, pp. 460 - 468.

[9] Alekha Kumar Mishra, Analysis of Secure Routing Scheme for MANET, Department of Computer Science Engineering, National Institute of Technology Rourkela, Rourkela-769008 (Orissa), India.

[10] Kun Wang, Meng Wu and Subin Shen, “A Trust Evaluation Method for Node Cooperation in Mobile AdHoc Networks”, International Conference on Information Technology: New Generations, Las Vegas, NV, 7-9 Apr. 2008, pp. 1000 – 1005.

[11] N. MirMotahhary, S.A.A. Fakoorian, H. Asadi and R. Khaniki, “Joint Optimization of Node Cooperation and Energy Saving in Wireless Sensor Networks with Multiple Access Channel Setting”, New Technologies, Mobility and Security, Tangier, 5-7 Nov. 2008, pp. 1-5.

[12] C.Sathiyakumar and K.Duraiswamy, “A Hybrid Approach for Node Cooperation based Clustering in Mobile ad hoc Networks”, Journal of Computer Science, Vol. 9, no. 2, pp. 147-154.