Trust-based Cluster head Selection Algorithm for Mobile Ad hoc Networks

Raihana Ferdous, Vallipuram Muthukkumarasamy, Elankayer Sithirasenan
Griffith University, Australia
Emails: raihana.ferdous@griffithuni.edu.au, v.muthu@griffith.edu.au, e.sithirasenan@griffith.edu.au

***Abstract*—Mobile Ad hoc Networks (MANETs) consist of a large number of relatively low-powered mobile nodes communicating in a network using radio signals. Clustering is one of the techniques used to manage data exchange amongst interacting nodes. Each group of nodes has one or more elected Cluster head(s), where all Cluster heads are interconnected for forming a communication backbone to transmit data. Moreover, Cluster heads should be capable of sustaining communication with limited energy sources for longer period of time. Misbehaving nodes and cluster heads can drain energy rapidly and reduce the total life span of the network. In this context, selection of best cluster heads with trusted information becomes critical for the overall performance. In this paper, we propose Cluster head(s) selection algorithm based on an efficient trust model. This algorithm aims to elect trustworthy stable cluster head(s) that can provide secure communication via cooperative nodes. Simulations were conducted to evaluate trusted Cluster head(s) in terms of clusters stability, longevity and throughput.**

I. Introduction

Mobile Ad Hoc Networks(MANETs) are completely autonomous wireless temporary networks established using a group of mobile nodes suitable for environments where no fixed network infrastructure is available. Unlike fixed hard-wired networks with physical defence at firewalls and gateways, attacks on MANETs can come from all directions and may target any node. Due to dynamic topology of the networks any security solution with static configuration are not sufficient. Any node must be prepared to operate in a mode that need not immediately trust other nodes without their trust information. If the trust relationship amongst the network nodes is available for every cooperating node, it will be much easier to select proper security measures to establish the required protection. Moreover, it will be more sensible to reject or ignore hostile service requests. As the overall environment in MANET is cooperative by default, these trust relationships are extremely susceptible to attacks. To avoid the overhead of handling the network as a whole, nodes are grouped into clusters. In this paper we introduce a trust based approach for Cluster head (TA) selection algorithm. Each cluster is nothing but a group of nodes which is headed by one or more node(s) known as Cluster head(s)(TAs). In our proposal Cluster head is elected by the member nodes in order to make the TA more stable depending upon some metrics. The Cluster head(s) selection is totally distributed and secured. The challenges can be handled by formalizing a trust relationship between the participating nodes within 1 hop distance away. To formalize the trust of a particular node, nodes monitor the behavior of other nodes and collect information from its neighbors and then take the decision about the node. We have used a quantitative trust evaluation algorithm at each node to evaluate the direct trust of its neighbor nodes.

The Node-based Trust Management(NTM) scheme is based on a Clustered mobile sensor network with backbone; it introduces a trust of a node within local management strategy with help from the mobile agents running on each node. That is, a node's trust-based information is stored as a history on the node itself and managed by the local mobile agent of the node.

This paper is organized as follows: Section II discusses related work in introducing trust and its associated issues in MANETs. Section III describes the work on the theory of trust formalization and node-based trust management (NTM) scheme. Section IV illustrates our proposed Cluster head selection procedure in NTM as well as route selection and updating trust information within NTM framework. Section V discusses simulation environment and results. Section VI describes the analysis of the results. Section VII concludes the paper.

II. Related Work

Low-Energy Adaptive Clustering Hierarchy (LEACH) has motivated the design of several other protocols [7] [14] which try to improve upon the Cluster head selection process by considering the residual energy of the nodes. Although LEACH is able to increase the network lifetime, there are still a number of issues to be investigated about the assumptions used in this protocol. LEACH assumes that all nodes can transmit with enough power to reach the Base Station if needed and that each node has computational power to support different MAC protocols. Therefore, it may not be applicable to networks deployed in large regions. It is not obvious how the number of predetermined Cluster heads is going to be uniformly distributed throughout the network. Therefore, there is a possibility that the elected Cluster heads will be concentrated in one part of the network. Hence, some nodes may not have any Cluster heads in their vicinity.

Trust-based Low Energy Adaptive Clustering Hierarchy(TLEACH) is a Wireless Sensor Networks(WSNs) trust protocol [15]. TLEACH contains two main components, the Monitoring Module and the Trust Evaluation Module.

Each node also maintains a Neighbor Situational Trust Table (NSTT) filled with trust value entries for each pair of node ids and situational operations. The trust update slot allows the Cluster head to share its trust values with its cluster members. TLEACH losses less data than LEACH because half of all data sent by cluster members is received by the gateway. TLEACH is, however, unable to stop the constant loss of data because of the lack of monitoring on the cluster head.

Li et al. [9] classify trust management as reputation-based framework and trust establishment framework. A reputation-based framework uses direct observation and second-hand information distributed among a network to evaluate other nodes. A trust establishment framework evaluates neighboring nodes based on direct observations while trust relations between two nodes with no prior direct interactions are built through a combination of opinions from intermediate nodes. Marti et al. [11] proposed mitigating routing misbehavior by detecting non-forwarding nodes and rating every path so that those nodes are avoided when the routes are recalculated. The resulting behavior is that non-routing nodes are not included in routing paths for non-cooperation but they still can ask others to forward their messages. This scheme detects the misbehavior but it does not isolate it. Therefore, in our system, we are considering only those nodes which are isolated by rating their trust value as low as 0 for non-cooperation.

There are several versions of the CONFIDANT protocol [2], [3] [4] and we summarize the most recent version here as CONFIDANT and CONFIDANT-extnd. Nodes using the CONFIDANT scheme rely on passive observation of all packets sent within a one-hop neighborhood to detect non-forwarding behavior. Each neighbor is initially allocated a null reputation value, and Bayesian theory is used to update the reputation values based on the nodes own observations. However, it is not clear whether a node broadcasts direct observations of only its current neighbors, or of all neighbors encountered during the nodes lifetime.

Hsieh et al. [16] use Cluster-based structure to ensure the security of wireless sensor networks which includes two modules: (1) the dynamic key authorization is adopted to prevent external malicious nodes from entering when a new Cluster is established or a new node joins in the cluster. (2) The nodes in the Cluster detect each other and different trust computing methods are formulated based on the different roles nodes take. The approach is difficult to implement and exists weak computing convergence.

Edith et al [12] discussed a trust model and a network model in order to enhance the security of public key certification. Their network model is based upon hierarchical organization or Clustering of the network by some Clustering algorithms. The authors perceived that such algorithms improve the security and the efficiency of the network. They assumed that the network has been divided into Clusters with unique IDs and trust model they [12] used is based upon the web-of-trust model the concept used in PGP [17]. In PGP, any user can act as the certifying authority. They define trust quantitatively as a continuous value between 0 and 1. Here, the authors did not discuss a mechanism for renewal and revocation of the certificates.

The following section describes the work [5], [6] related to the trust formalization and how this formalized notion helps to build our NTM scheme in MANETs.

III. Theory of Trust Formalization of NTM

This section mainly describes the trust formalization [5], [6] so that the analysis of Node-based Trust Management (NTM) can be developed. These properties of trust will be defined in later section. In NTM scheme, we need to compute TEs (Trust Evaluators) by grasping the TRUST-VALUE from equation 1. According to the Watchdog and Pathrater schemes [11], utilized for cooperation of nodes in ad hoc networks. Therefore, a node n_i's trust on another node n_j can be defined as:

$$T_{n_i,n_j} = \alpha_1 {}_{n_i}T_s^{n_j} + \alpha_2 {}_{n_i}T^{n_j}o \tag{1}$$

In the above equation, T_{n_i,n_j} is evaluated as a function of two parameters:

- ${}_{n_i}T_s^{n_j}$: Node n_i's self evaluated trust on n_j; n_i computes this by directly monitoring n_j.
- ${}_{n_i}T^{n_j}o$: Weighted sum of other nodes' trust on n_j evaluated by n_i.

In eq. (1), α_1 and α_2 are weighting factors such that $\alpha_1 + \alpha_2 = 1$. Thus, by varying α_1 and α_2, n_i can vary the weight of self evaluated vs. others trust in calculating its total trust on n_j. Here, $0 \leq T_{n_i,n_j,n_i}T_s^{n_j},{}_{n_i}T^{n_j}o \leq 1$, and thus eq. (1) is normalized.

Node n_i computes this value by directly monitoring n_j when n_j is in its radio range. As it mentioned earlier [5] that any node wishes to send messages to a distant node, sends the ROUTE REQUEST(RTREQ) to all the neighboring nodes within the Cluster. The ROUTE-REPLY(RTREP) obtained from its neighbors are sorted by trust ratings. The source selects the most trusted path. If its one hop neighbor node is a friend, then that path is chosen for message transfer.

A. An Overview of the node

The NTM is based on a Clustered MANET with backbone, and its core is a mobile node system. Differing from traditional trust and reputation management systems, NTM requires that a node's trust information to be stored in the forms of Trust evaluators (TEs) by the node itself. Obviously, nodes cannot manage and compute their own trust. So, NTM further requires that every node locally hold a mobile node that is in charge of administrating the trust of its hosting node. In this sense, mobile nodes provide nodes a "one-to-one" trust management service.

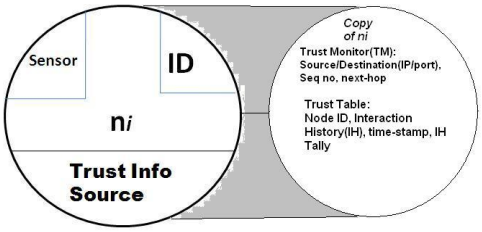

Figure 1. A node in NTM

Table I
A TABLE OF TETBL OF NODE n_i

ID	CNTXT	EVAL	TSTMP	COUNTR
$ID(n_i)$	Context	t_{ij}	T	1

B. System Architecture

The architecture of NTM consists of three key segments: Node Initiators (NIs), Trust Monitors(TMs),and Trust Evaluators(TEs). Each node of NTM consists of four components: wireless sensor, ID of the node, Trust Info-score and Context (Figure-1). A TM is a mobile agent generated by the NI. It is designed to be distributed into every node and to provide its hosting node with a trust management service. Each node will hold a copy of the TM's current version. For an arbitrary node n_i, its copy TM, $TM(n_i)$, locally maintains three data structures, i.e. a trust evaluation table TETBL, an interaction history buffer HB and a message counter COUNTR. The trust evaluations that n_i recently made on other nodes are kept in TETBL, while the TEs issued to n_i by the local copy TMs of other nodes are also stored in TETBL.

As illustrated in Table I, TETBL is composed of five fields, ID, CNTXT, EVAL, TSTMP, COUNTR among which ID and CNTXT together constitute the primary key of the table. Field ID contains the IDs of the evaluated nodes; field CNTXT implies trust contexts; and field EVAL stores the trust evaluation values; field TSTMP holds the time when evaluations are made. For any node n_i, field CNTXT implies trust contexts. Field TSTMP holds the time when TEs are issued, while field COUNTR reflects how many times a TE is acknowledged. A copy TM stays on its host until it is replaced by the copy of a higher-version TM, and in the meantime it offers its host the trust management service. When TM replacement takes place, the new local TM will take over all the data structures maintained by the old one and reset COUNTR to 0. *Trust Evaluators(TEs)*: A Trust Evaluator is a segment of data that is organized with a special structure and issued by the copy TM of a node *(sender)* to another node *(receiver)*. It is stored in the TETBL on its receiver node. Considering any two nodes n_i and n_j, the TE issued by $TM(n_i)$ to n_j under context, **Context** is defined as:

$$TE(n_i, n_j, CNTXT) = EVAL_{SK}(D) \tag{2}$$

where D = (ID(n$_i$), ID(n_j),CNTXT,T,t$_{i,j}$) and T is a time-stamp implying the time when the TE is issued. From the above definition, we can see that a TE implicitly indicates the temporal property of trust by the use of a time-stamp T. TE is driven by transactions, and it involves message transmission between the copy of TMs of the sender and receiver. The execution of NTM involves three phases: *network formatting phase*, the *Trust Management interaction routine phase* and finally the *security analysis phase*. As soon as NTM starts, the network formatting phase is initiated.
Specifically, it is possible that some nodes do not yet have a local copy of TM when they are asked by other nodes for TEs. Clearly, the asynchronous execution may lead to the failure of the trust management service. The trust value acquisition service consists of three algorithms stated in [5], [6].In the trust management interaction routine, each intermediate node accommodates incoming TRUST-INFO in proper buffers (HBs). Upon receiving the first INFO, the node will calculate the appropriate time duration for holding INFO in the buffer before forwarding it to the next node.
NTM classifies each incoming INFO as based on each INFO's arrival time, and adaptively determine a suitable due time for each INFO individually. Whether INFO is early, in time, or late depends on its relative delay.

IV. PROPOSED CLUSTER HEAD SELECTION PROCEDURE IN NTM

In this paper, we propose that the entire network be divided into hierarchical group of clusters. We assume that nodes are location-unware i.e. not equipped with GPS, they are left unattended at the beginning so no need for battery re-charge and all nodes are given initial trust value to start with i.e. 0.5.
In MANET, we denote the set of all nodes as $N = n_1, n_2, ..., n_i$ where $i \geq 2$. After deployment, pairs of nodes $n_i, n_j \subseteq N$ may interact with each other. Such interaction is regarded as successful if n_i and n_j both cooperate and denoted as unsuccessful if either of the nodes does not cooperate. The interaction history(IH) of observed outcome between n_i and n_j, from the perspective of n_i, is recorded at any given time *t* as a tuple:

$$IH^t_{n_{ij}} = (Suc^t_{n_{ij}} + U^t_{n_{ij}}) \tag{3}$$

Where $Suc^t_{n_{ij}}$ is the number of successful interaction and $U^t_{n_{ij}}$ is the number of unsuccessful interaction between n_i and n_j. In the node discovery process, which immediately follows deployment, each node periodically, in the order of seconds, broadcasts one-hop hello packets to discover its neighbors. On the reception of a hello message from node n_i, node n_j replies with an authenticated message using the pairwise key. Embedded in the reply are n_j 's node ID

along with time stamp and location information. If node n_j is verified to be authentic, then it is recorded in n neighbors list (TETBL), and its trust value is initialized.

A. Cluster Formation

After deployment, the nodes broadcast their $ID(n_i)$ and TRUST value to their neighbors along with the REQ/REPLY flag. When the participating the nodes have discovered their neighbors, they exchange information about the number of one hop neighbors. The node which has maximum one hop neighbors from the trust interaction table is selected as the TA. Other nodes become members of the Cluster or local nodes. The nodes update the trust values accordingly. A circle is formed with a fixed radius by selecting (either randomly or with highest cooperating neighbor density within 1 hop distance) a node as center and an arbitrary small length as radius. Center of the new circle is computed as the mean of the points within the circle while the radius in increased by the distance of two successive centers. The nodes reply back and in this way Clusters are formed in the network as shown in Figure-2 and Algorithm-1. In this manner Clusters are formed in the network. The entire MANET is hierarchical in nature and following sequence is observed network-group-Cluster-Cluster node.

Algorithm 1: Cluster Formation algorithm in NTM

Input: Set of nodes
Output: Set of clusters
Begin Cluster =1 /* represent cluster number 1 */
Repeat
Select a node n_i which is 1 hop distance apart from other participating nodes with a small length d1 randomly
Do
N = n_i ; d= d1
Draw a circle with n_i as center and d as radius
Compute new radius $(d1) = d + |n_i - n_j|$
while $n_i \neq n_j$
Cluster-1 is formed with cooperating nodes lying within the circle;
End

B. Cluster head selection algorithm

In this section we consider the selection of Cluster heads(TAs) in a MANET of n nodes such that every node in this network is within distance h hops of a TA, for a given TRUST-VALUE. Here, in our NTM model, the Cluster lifetime denotes the time from the point a node is elected as Cluster head until the point a node changes its status to normal node. It should be noted that the Cluster lifetime is dependent on mobility issues, the Cluster lifetime in MANETs depends on link stability. In our simulation

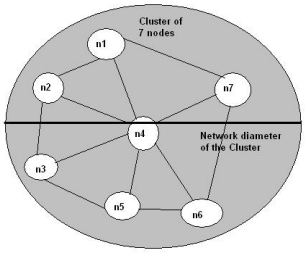

Figure 2. Cluster Formation of 7 nodes

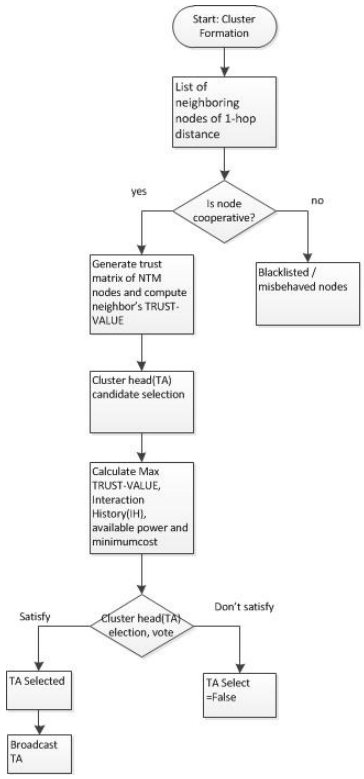

Figure 3. Cluster head(TA) selection Flow Chart Diagram

model(using NS2) a Clustering message is sent every 3 seconds. Thus, a neighbor node is kept in the neighbor table for $3 * COUNTR$ seconds and discarded if there is no further Clustering message received. Initially, the Interaction History (IH) for all nodes has been considered as null or ≥ 1. Algorithm 1 depicts the Cluster head(s) selection process as well as a flow chart diagram has been shown in figure 3. From equation (1) TRUST-VALUE can be further evaluated by

$$T_{ij} = \frac{\sum_{n=i}^{n=0} T_{ij}}{IH} \tag{4}$$

where $i, j \in nodes$; T_{ij} is node i's TRUST-VALUE for node j. Due to the dynamic changes in the topology of network, the Cluster structure is updated from time to time. It should

be noted that whenever a node forwards a packet, it loses some amount of energy whose amount depends on factors such as the nature of packets, their size, access frequency, and the distance between the nodes. Therefore we have assumed individual energy power in considering the path, that is, if there is a path with a node having very low energy level, then the available power function does not select that path, irrespective of whether or not that path is time efficient.

Algorithm 2: Cluster head (TA) Selection algorithm in NTM

$TA_{cur} \longleftarrow 0$
$TA_{prev} \longleftarrow 0$
$Time_{prev} \longleftarrow 0$
now() $\longleftarrow 0$
$Time - OUT_{loop} \longleftarrow$3*COUNTR
From equation (1) TRUST-VALUE can be further evaluated by **equation 5**
Interaction history$(IH) \geq 0$
while $Time_{prev} \leq now()$ **or** $TRUST - VALUE(TA_{prev}) \leq 1$ = true **do**
    TA_{prev} remains as Cluster head
end while
if $TRUST - VALUE(TA_{prev}) = TRUST - VALUE(TA_{cur})$ **and** $IH(TA_{prev}) = IH(TA_{cur})$ **then**
    both TA_{prev} and TA_{cur} remain as Cluster heads
else
    select new Cluster head(s)
end if

C. Routing Information for "NEW" node joining the Cluster

When a node joins a mobile ad hoc network (MANET), it receives a certificate from a TA. It also contains a TRUST-VALUE that tells the maximum trust that this entity will have whereas it bears the certificate in question. TA are responsible to translate nodes behavior in new trust values and also to inform the new trust information amongst the other nodes of the Cluster shown in Figure 4. However the following steps should be in place for a "New" node joining in to the network:

- Step 1: After elected as TA, each TA starts to broadcast TA beacon and attracts some nodes to join its cluster.
- Step 2: As the node n_k gets the TA beacon, it sends REQ beacon to join the network with its public key.
- Step 3: TA checks whether it is a duplicate message or not. If it is not a duplicate, TA stores the public key of n_k as its id and generates a pairwise shared key to communicate between TA and n_k. Also sends a secret key(SK) for secure intra cluster communication.
- Step 4: Initially TA gives the node as NEW status and allows it to register subject to periodic review of its recommendation.
- Step 5: TA executes the Algorithm and calculates its direct trust about n_k. TA asks its one hop members of n_k to send their recommendation for n_k.
- Step 6: If Trust is higher than a threshold(0.5), TA sends a trust certificate CERT. Thus n_k becomes a Trusted Member of the cluster.

D. Routing Information for "Inter-Cluster" Communication

It should be noted that we assume all the TAs are being elected as most trusted nodes and interact with other TAs for any updated information. Therefore, all TAs together form a higher-level network, upon which Clustering can again be applied. We consider the case (Figure 4) where node N-11 wants to broadcast a message to N-21 of its neighbor. To be able to authenticate that the packet originated from node N-11, node N-21 sends the request to the Cluster head TA-2. Cluster head TA-2 then verifies with the other Cluster head TA-1 to whom N-11 belongs to. If TA-1 confirms the authenticity of N-11 to TA-2, TA-2 then relays this message to N-21 to confirm whether N-11 trustworthy or not. This two-way verification hinders any misbehaving node to perform any attack on MANET environment.
The following steps need to be performed while "Inter-Cluster head " communications:

- Step 1: n_k sends the ROUTE REQUEST(RTREQ)to TA-1.
- Step 2: TA-1 checks the status of the n_k; if n_k is not Trusted, TA-1 just drops the request and generates a message. If n_k is trusted, TA-1 generates a OK message.
- Step 3: n_k starts Route discovery to get n_i. Do Step 4 to Step 6, if n_j under TA-1 responds in positive. If no member node replies do Step 7 to Step 9.
- Step 4: n_k sends the route to TA-1. TA-1 checks the status of n_j; if it is trusted, the TA-1 generates a session key, $K_{session}$ for inter cluster communication for n_j.
- Step 5: n_j gives reply to n_k with the public key of n_i. n_k encrypts the Ks with the public key of n_i and encrypts the message with $K_{session}$ and sends via n_j.
- Step 6: n_j gets the message and generates a session key with n_i and encrypts the total message with that session key and sends the message to n_i.
- Step 7: n_k sends the message to TA-1. TA-1 multicasts reveal-recommendation query to all it neighbor TAs for having a communication to TA-2.
- Step 8: If TA-2 replies or any other TA replies that it can sense TA-2, TA-1 initiates a route discovery request and asks for the public key of n_i.
- Step 9: n_j. getting the public key TA-1 encrypts the $K_{session}$ with the public key of n_i and encrypts the message with $K_{session}$ and sends over the discovered route.
- Step 10: After a successful receipt n_i sends an acknowledgement via the same path.

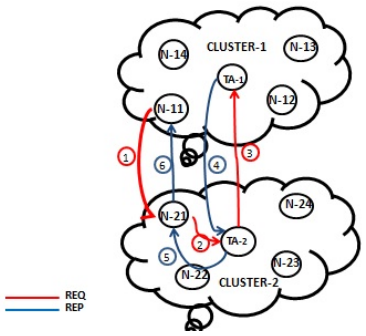

Figure 4. Node-based Secured Interactions

Therefore, trust regarding each node may rise or fall according to its behavior.

E. Cluster head Maintanance: Updating of TETBL in NTM

The updating of Trust Information in NTM TETBL requires trust infrastructure security layer, which represents a fundamental building block of the network, consisting of the basic relationships between the nodes. When a trust relationship has been established with a node, it is necessary to update the level of trust associated with that node on a continuous basis. Since TRUST-VALUEs are maintained in TETBL of NTM node, these values indicate how much the node can trust its neighbors to send accurate information. If received information corresponds to the node's own cooperative view in a given time frame, only then the node can increase the TRUST-VALUE of the source informant. Otherwise, the TRUST-VALUE is decreased.

1) Trust Decay: Initially, let node n_i in Cluster 1 has trust value on node n_j is $T_{n_{ij}}(t_1)$ at t_1 time. After a certain period, node n_j may leave for another cluster network. Therefore node n_j is out of radio range of node n_i due to node mobility nature in MANET.. At time t_2, node n_j joins in Cluster 1 again. The TRUST-VALUE of node n_j decays over this time gap. Let $T_{n_{ij}}(t_2)$ is the new TRUST-VALUE of n_j given by n_i at time t_2, such that $T_{n_{ij}}(t_1) \succ \mathrm{T}_{n_{ij}}(t_2)$. It defines

$$T_{n_{ij}}(t_2) = T_{n_{ij}}(t_1) * exp[-(T_{n_{ij}}(t_1)\Delta t)]^{2k} \qquad (5)$$

where $\Delta t = t_2 - t_1$ and k is an integer such that $k \geq 1$.

2) Trust Increase: Each NTM node consists of a TETBL which also contains TRUST-INFO. TRUST-INFO is a combination of recommendation, interaction history(IH), TRUST-VALUE(range from 0.0 to 1.0). Recommendation is regarded as "trust certificate" given by other nodes while interaction. It can be used for evaluating other nodes' ability to execute an expected action and a node can take advantage of this recommendation information to make decisions. IF a node's i.e. n_i, interaction history(IH) shows that it has been cooperative with other neighboring nodes while interaction, TRUST-VALUE is increased for n_i.
In this paper, the TRUST-VALUE is a continuous real number[0.0, 1.0]. This definition satisfies the following properties:

- when $T_{n_{ij}=1}$, n_i trusts n_j the most and the trust value is 1.
- when $T_{n_{ij}=0}$, n_i distrusts n_j the most and the trust value is 0.
- when $T_{n_{ij}=0.5}$, n_i neither fully trusts nor distrusts n_j and is regarded as 'Threshold value'.

Therefore, when the TRUST-INFO entities(Recommendation, IH and TRUST-VALUE) of n_i are all positively verified and successfull, then the overall TRUST-VALUE of n_i are increased at the time instance (t) as-

$$T_{n_i}(t) = \sum_{i=0.5}^{i=1} T_{n_i} + \Delta t + \beta_{n_i} \qquad (6)$$

where β_{n_i} is the step value for node $n - i$, which can be assigned as a small fractional value during simulation and where $0.5 \leq T_{n_i}(t) \leq 1$.

3) Cluster head(TA) Longevity: Proposed TA selection algorithm also deals with the longevity of the mobile network with nodes' executing operations(interacting with each other). As we have stated before, each node is equipped with identical battery-life. The battery power is consumed to transmit over a distance. therefore, the only failure is due to battery power outage. Typically, the nodes in MANET broadcast infrequently and over a short distances. Where as TAs broadcast frequently over longer distances. Therefore Cluster heads would typically run out of battery and die sooner than the Cluster member nodes. Once a TA dies, the Cluster head selection algorithm back in action again. The cycle continues until very last node of that Cluster runout of power.

V. Simulation and Results

We used Network Simulator-2 (ns2) [10] as simulation tool to analyze the performances of the Cluster head (TA) selection algorithm. This includes: trust evaluation of cooperating nodes, non-cooperating nodes as well as their influence of factors on the trust evaluation. The proposed algorithm and claims are validated using simulation results.

A. Environment

The simulation experiments are carried out in LINUX (UBANTU 10.10). In a typical simulation, our program generates a random network topology according to some input TRUST VALUEs. Then the TA selection algorithms are executed by the nodes on this network topology and the parameters of interest are reported.

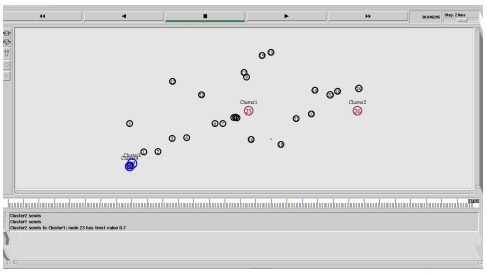

Figure 5. Simulation results in NAM

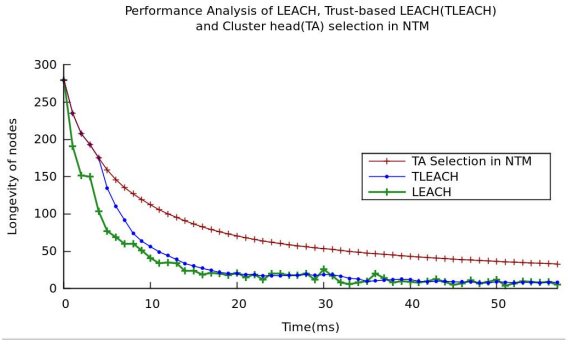

Figure 6. Performance Analysis of three Algorithms

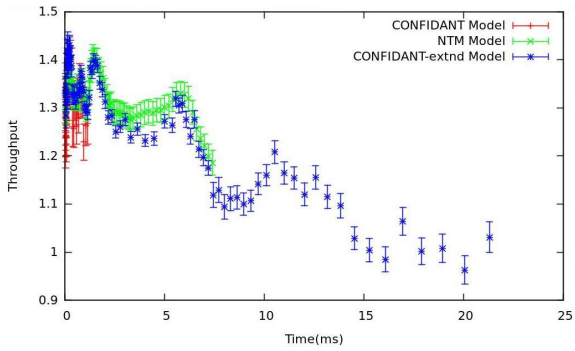

Figure 7. Comparisons between NTM, CONFIDANT and CONFIDANT-extnd Trust Models

B. Traffic Model

Continuous bit rate (CBR) traffic sources are used. The source-destination pairs are spread randomly over the network. Only 512-byte data packets are used. The number of source-destination pairs and the packet sending rate in each pair is varied to change the offered load in the network.

C. Mobility Model

The mobility model uses the random waypoint model in a rectangular field. Simulations are run for 30 seconds. Identical mobility and traffic scenarios are used across protocols to gather fair results. Mobility models were created for the simulations using 28 nodes, with pause times of 5.05 seconds, maximum speed of 20 m/s, topology boundary of $500m \times 500m$ and simulation time of 30 secs. It should be noted that as the transmission range increases, the Cluster head covers more number of nodes that are within its transmission range. Therefore, the number of Clusters decreases as the transmission range increases.

D. Results

The performance of the proposed algorithm is evaluated. Firstly, we assume the actions of each node in network are normal. When the trust evaluation system tends to be stable, TRUST VALUE of nodes increases slowly. After a few successful interactions, nodes' TRUST VALUE increases gradually. It should be noted that in our simulation in ns2, TRUST-VALUE is incremented by 0.10 every time there is an interaction occurred in between cooperating nodes until they reach to their highest TRUST-VALUE 1.
Packet delivery ratio (PDR) at time t is defined by:

$$PDR = \frac{\sum Pckt_{recv}}{\sum Pckt_{sent}} \times 100 \qquad (7)$$

Simulations aim at showing, for the trust-based, energy-efficient and the distance-constrained Cluster head selection, the parameters that influence the network overhead such as longevity of the nodes. We demonstrate that how the lifetime of the entire network can be extended compared with the existing clustering protocols such as LEACH and TLEACH. Therefore simulation results showed in Figure 6 illustrate that proposed TA selection procedure in NTM out performs both LEACH and TLEACH in terms of network lifetime.

VI. Analysis and Discussion

In this study, we have implemented the algorithms for network Cluster formation for MANETs. In our approach, a node has to gather information from its neighboring nodes to eshtablish the trust for itself. Therefore, in this research we investigate the formation of Clusters based on the trust values among the nodes. We believe that it takes time for a node to collect enough data and to identify its neighboring nodes as malicious. From the experiment result about mobility, we found that most of the nodes stay in the same Cluster for few cycles until they reached the trust value of 1.
The packet delivery ratio changes due to varying the percentage of both cooperating and non-cooperating (malicious) nodes. Packet delivery ratio of cooperating nodes is greater than that of non-cooperating nodes. When there are 85% cooperative nodes in the network, the packet delivery ratio for all nodes is 37% because a portion of the communication happens between nodes that are within each other's radio range. Figure 7 also shows the comparisons of throughput obtained using NTM, CONFIDANT and CONFIDANT-extnd Trust models. Results show that NTM as a trust model similar to CONFIDANT and CONFIDANT-extnd, but NTM primarily differs from CONFIDANT by enabling every node

to broadcast its reputation to all neighbouring nodes of 1 hop distance. NTM, in this case, performs better than CONFIDANT-extnd in terms of average end-to-end delay, packet successful delivery ratio and throughput.
The proposed algorithm further depicts that if there are several Cluster heads in the neighborhood, the node should select the one that has the largest Cluster members as its Cluster head, and it becomes a member of the selected Cluster. If there is no Cluster head in the neighborhood, the node elects a new Cluster head(TA) amongst its neighboring nodes.

VII. Conclusions

Introducing clustering into the network topology reduces the communication overheads in MANETs. In this paper, we have presented selected clustering protocols for MANETs that describe various modifications carried over the Node based Trust Management Scheme (NTM). The Cluster head selection algorithm is formulated by considering mobility of nodes. The nodes themselves determine whether they become Cluster heads using TRUST-VALUE. Experiment results reveal proposed Cluster head selection procedure in NTM, out performs both LEACH and TLEACH in terms of network lifetime. As a trust model, NTM performs better than CONFIDANT-extnd in terms of packet successful delivery ratio and throughput. However, there are a couple of limitations in this approach. The way the messages passed through may overload the Cluster head, creating a bottleneck due to additional message exchanges. Another possible limitation is the way that the message authentication between intermediate Cluster heads are treated, where there can be a delay in identifying a malicious neighboring node(s). Moreover, we have not investigated some of the major security challenges for route discovery in MANETs yet. However, we do believe that the benefits pointed out in analysis are significant and promising with better performance measures.

References

[1] M. Bechler, H.-J. Hof, D. Kraft, F. Phlke and L. Wolf. *A Cluster-Based Security Architecture for Ad Hoc Networks*. I Proceedings of IEEE INFOCOM, vol 4, Mar 2004, pp 2393-2403.

[2] S. Buchegger and J.-Y. Le Boudec. *Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks*. In Proceedings of the 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing PDP, Las Palmas de Gran Canaria, Canary Island, Spain, January 9-11, 2002, pages 403-410. Euromicro, Jan 2002.

[3] S. Buchegger and J.-Y. Le Boudec. *A robust reputation system for P2P and mobile ad hoc networks*. In Proceedings of the Second Workshop on the Economics of Peer-to-Peer Systems, P2PEcon 2004, Cambridge, MA, US, June 4-5, 2004, Harvard University Press, Jun 2004.

[4] S. Buchegger and J.-Y. Le Boudec. *Self-policing mobile ad hoc networks by reputation systems*. Communications Magazine, IEEE, 43(7):101107, Jul 2005.

[5] R. Ferdous, V. Muthukkumarasamy and A. Sattar, *Trust Management Scheme for Mobile ad hoc Networks*, Proceedings of the 10th IEEE International Conference on Computer and Information Technology (CIT-2010), June-July 2010, Bradford, U.K.

[6] R. Ferdous, V. Muthukkumarasamy and A. Sattar, *A Node-based Trust Management Scheme for Mobile ad hoc Networks*, Proceedings of the 4th IEEE International Conference on Network and System Security (NSS 2010), Sept 1-3, 2010, Melbourne, Australia.

[7] M. J. Handy, M. Haase and D. Timmermann, *Low energy adaptive clustering hierarchy with deterministic cluster-head selection*, in Proc. 4th IEEE International Workshop on Mobile and Wireless Communications Network (MWCN '02), Stockholm, Sweden, September 2002, pp. 368-372.

[8] P. Krishna, M. Chatterjee, N. Vaidya and D. Pradhan. *A Cluster-based Approach for Routing in ad hoc Networks*. Proc 2nd Symposium on Mobile and Location-Independent Computing. Apr. 1995.

[9] J. Li, R. Li and J. Kato, *Future Trust Management Framework for Mobile Ad Hoc Networks: Security in Mobile Ad Hoc Networks*, IEEE Communications Magazine, vol. 46, no. 4, Apr. 2008, pp. 108-114.

[10] S. McCanne and S. Floyd. ns–Network Simulator. http://www-mash.cs.berkeley.edu/ns/.

[11] S. Marti, T.J. Giuli, K. Lai, and M. Baker. *Mitigating Routing Misbehavior in Mobile Ad Hoc Networks*. Mobicom 2000, August 2000, pp. 255-265.

[12] C. H. Ngai Edith and R. Lyu Michael. *Trust- and Clustering-Based Authentication Services in Mobile Ad Hoc Networks*, 24th International Conference on Distributed Computing Systems Workshops - W4: MDC (ICDCSW'04), Hachioji, Tokyo, Japan, 2004. Vol 3/23-24.

[13] E.M. Royer and C.E. Perkins. *Ad-hoc on-demand distance vector routing*. Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, 1999, pp.90.

[14] I. Saha Misra, S. Dolui and A. Das, *Enhanced-Efficient Adaptive Clustering Protocol for distributed sensor networks*, ICON 2005

[15] F. Song and B. Zhao. *Trust-Based LEACH Protocol for Wireless Sensor Networks*. In Proceedings of the 2008 Second international Conference on Future Generation Communication and Networking - Volume 01 (December 13 - 15, 2008). FGCN. IEEE Computer Society, Washington, DC, pp-202-207.

[16] M.Y. Hsieh, Y.M. Huang and H.C. Chao. *Adaptive Security Design with Malicious Node Detection in Cluster-Based Sensor Networks*. Comput. Commun. 2007,vol- 30,pp 2385-2400.

[17] P.R. Zimmermann, The Official PGP Users Guide, MIT Press, 1995.