A Node-based Trust Management Scheme for Mobile Ad-Hoc Networks

2010 Fourth International Conference on Network and System Security

A Node-based Trust Management Scheme for Mobile Ad-Hoc Networks

Raihana Ferdous, Vallipuram Muthukkumarasamy, Abdul Sattar
Institute for Integrated and Intelligent Systems
Griffith University, Australia
Email: raihana.ferdous@student.griffith.edu.au, v.muthu@griffith.edu.au, a.sattar@griffith.edu.au

***Abstract*—The inherent freedom in self-organized mobile ad-hoc networks (MANETs) introduces challenges for trust management; particularly when nodes do not have any prior knowledge of each other. Furthermore in MANETs, the nodes themselves should be responsible for their own security. We propose a novel approach for trust management in MANETs that is based on the nodes' own responsibility of building their trust level and node-level trust monitoring. The main contribution of this work is in the introduction of a Node-based Trust Management (NTM) scheme in MANET based on the assumption that individual nodes are themselves responsible for their own trust level. We explore and develop the mathematical framework of trust in NTM. Finally, in this context, we demonstrate our scheme with notations, algorithms, analytical model and prove of its correctness.**

I. Introduction

Mobile ad-hoc networks (MANETs) are dynamically configured, multi-hop wireless networks with varying topology. Due to the unique characteristics of MANETs and the inherent unreliable nature of the wireless medium, the concept of trust in MANETs should be carefully defined. A trust management framework for MANETs cannot assume that all nodes are cooperative. In resource-restricted environments, selfishness is more likely to be prevalent over cooperation. Trust is also context-dependent, i.e. *A* may trust *B* as a doctor but not as a plumber.

The main problems that we address in this paper are the following: (a) to define a metric that the nodes can use to make decisions on whether to establish keys with other nodes in an ad-hoc network, given that the infrastructure for establishing such keys exists, and (b) to define a trust management scheme in which nodes in a MANET can securely group together in order to trust each other. We also propose a node-based trust management system architecture, the relevant algorithms and proof of correctness to analyse the phases of this scheme.

Our proposed management scheme is based on a clustered wireless mobile sensor network with backbone and on a mobile agent system; 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 depicts some related work in introducing trust and security 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 Scheme with notations and definitions along with proof of correctness . Section V depicts the analytical part of NTM with the system architecture and relevant algorithms. Finally section VI concludes the paper.

II. Related Work

The idea of using trust to mitigate security threats has been an important area of research [23]. Trust establishment and management between entities (nodes or agents) can be done through a central trusted authority or in a distributed fashion by nodes [2], by a combination of both. Related work in this area [7], [24], [14], employ all these approaches. For example, Zhou et al. [12] proposed the idea of utilizing threshold cryptography to distribute trust in ad-hoc networks, Davis [4] proposed the use of certificates based on hierarchical trust model to manage trust, and Eschenauer et al. [11] contrast between trust establishment in ad-hoc networks and the Internet. Some researchers have shown that rating nodes' trust level is an effective approach in distributed environments to improve security [1] to support decision-making[21][27] and to promote node collaboration [19].

Existing trust management schemes like [13], [18] were designed originally for wired networks (e.g., P2P), and are thus not directly suitable for wireless sensor networks, where nodes have resource constraints. The schemes in [20], [9] are developed for wireless networks, but they focus mostly on trust and reputation modelling and seldom emphasize on the network performance issues. The most commonly used approaches by these schemes for acquiring reputation can be classified into two groups; on-demand and periodical. Although the scheme presented in [20] restricts flooding to a subset of nodes, how to determine the subset such that it covers all the nodes (or a sufficient number of nodes) holding the required trust information becomes a problem.

Li et al.[10] classify trust management as reputation-based framework and trust establishment framework. According to Li et al. [8], trust management is classified as evidence-based trust management and monitoring-based trust management.

The new metric of trust represented in this paper differs

978-0-7695-4159-4/10 $26.00 © 2010 IEEE
DOI 10.1109/NSS.2010.67

from the previous trust models, described in this section, in the sense that it considers a copy of each node within the environment for the trust monitoring aspect. It should be noted that only two end nodes (source and destination) collect evidences and update their opinion on the trustworthiness of the communication path. In this context we demonstrate with new notations, algorithms, analytical model and prove of its correctness. Therefore, firstly, we need to determine how the trust notion can be defined amongst mobile nodes. The following section depicts our work [16]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 of our previous work[16], [17] so that the analysis of our proposed Node-based Trust Management (NTM) can be developed. It should be noted that we assume *trust is transitive* and *trust values* are represented as *binary* rather than as a continuous-valued variable. 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 2. Our schemes draw ideas from the Watchdog and Pathrater schemes [22], utilized for cooperation of nodes in ad-hoc networks. We define a node n_i's trust on another node n_j 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. Here, the common-wisdom is to formalize Trust, as a notion, to be stochastic. We do not know of a justification to up-front impose this restriction. In contrast, we define only the matrix of weights to be stochastic (this is exactly the meaning of weighted average) and allow trust to have any value in the real interval $[0, 1]$. This change is sufficient to unmask the above phenomenon. The weighted average is designed to give a calculated recommendation on how much the source node should trust the destination node.

Node n_i computes this value by directly monitoring n_j when n_j is in its radio range. We define ${}_{n_i}T_s^{n_j}$ as:

$${}_{n_i}T_s^{n_j} = f(\Phi, \Omega) \tag{2}$$

Node n_i's self trust on n_j is a function (f) of traffic statistic functions Φ and Ω computed by monitoring n_j. Precise definition of f can be implementation dependent. We assume f to be a weighted sum of Φ and Ω . Here, Φ is a function of monitored traffic statistics pertaining purely to traffic volume and Ω is a function of monitored traffic statistics pertaining to information integrity. Lee et al. [26] compile node monitoring statistics for one hop neighbours in ad-hoc networks. Here the weighting is a function, *f*, of magnitude as means of balancing defamation against subjective expression. 1 Based on these monitored statistics we define Φ and Ω as:

$$\Phi = g(\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6) \tag{3}$$

$$\Omega = h(\lambda_1, \lambda_2) \tag{4}$$

Here *g* and *h* can again be defined based on the implementation. Like *f*, we assume them to be weighted summation of their constituent parameters. These parameters are defined below:

γ_1: packets sent by n_j to n_i that are dropped by n_j
γ_2: total packets dropped by n_j
γ_3: packets dropped by n_j due to congestion
γ_4: packets dropped by n_j due to unknown reasons
γ_5: n_i's assessment of n_j's priority to n_j's self packets vs. all other nodes' packets
γ_6: packet forwarding delay by n_j
λ_1: packets misrouted by n_j
λ_2: packets falsely injected by n_j

In the representation ${}_{n_i}T^{n_j}o$, O is the set of other nodes, whose trust on n_j is utilized by n_i in evaluating its own trust on n_j. O is defined as:
$O = \forall$ node $o \in O \Rightarrow o$ is in the range of both n_j and n_i, and $\exists T_{no}, s.t. T_{no} \geq$ "*good*".
Here "good" is a threshold value for demarcating Unknown and Good trust-regions.
Now, in traditional routing protocols, choosing where to forward a message is usually a simple task; the message is sent to the neighbour that has the path to the destination with the lowest cost (often the shortest path). Normally the message is also only sent to a single node since the reliability of paths is relatively high. In this paper, we adopt the concept of DSR[5],[6] which is a routing protocol and is designed for use in a multi-hop environment like wireless mobile ad-hoc networks. It allows mobile nodes to organize and configure themselves to form connections between them without any aid of an existing infrastructure or administration. As it mentioned earlier that any node wishes to send messages to a distant node, sends the ROUTE REQUEST(RTREQ) to all the neighbouring nodes. The ROUTE REPLY(RTREP) obtained from its neighbours are sorted by trust ratings. The source selects the most trusted path. If its one-hop neighbour node is an acquaintance and if the one hop neighbour of the second best path is a Trustworthy then ***T*** is chosen otherwise it is ***U*** as depicted on the table 1. Similarly an optimal path is chosen based on the degree of trustworthiness existing between the neighbour nodes. The source selects the shortest and the

TABLE I
PATH CHOSEN IN PROPOSED SCHEME

Next hop neighbour in the best path P1	T	U	T
Next hop neighbour in the best path P2	U	U	T

TABLE II
PROPOSED NOTATIONS FOR NTM

NAME	DESCRIPTION
NTM	Node-based Trust Management
n_i	A node in the network
$CNTXT_i$	A given context
$ID(n_i)$	ID of node n_i
SK	A symmetric secret key held by TM
COUNTR	Message counter
HB	Interaction History stored in a Buffer
TETBL	Trust evaluation Table
TEs	Trust evaluators
INFO	Trust Information

next shortest path. Whenever a neighbouring node is rated as trustworthy, the message transfer is done immediately. This eliminates the overhead of invoking the trust estimator between trusted partners. If it is an acquaintance or stranger, transfer is done based on the ratings. This protocol will converge to the DSR protocol if all the nodes in the ad-hoc network are being rated as trustworthy, ***T***.

Trust information is usually requested by nodes before they start communicating with each other, trust management schemes with poor trust are not acceptable in situations with strict real-time requirements, like battlefields and emergency rescue services. Therefore, we introduced a novel node-based trust management scheme (NTM) for MANETs [17]. The main objective of the NTM is to effectively manage trust and reputation with minimal overhead in terms of extra messages and time delay. The notations to be used for describing the NTM can be found in Table II.

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 and reputation. So, NTM further requires that every node locally hold a mobile node that is in charge of administrating the trust and reputation of its hosting node. In this sense, mobile nodes provide nodes a "one-to-one" trust and reputation management service.

B. NTM Network Model

In this paper, we use a network model based on sufficient backbone nodes with multiple long-range radios that are randomly scattered in the MANET. Every node has a unique ID by which it can be distinguished from others. Through a secure routing protocol, all the nodes

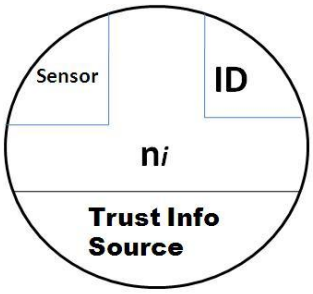

Fig. 1. A node in NTM

(including backbone nodes) together compose a low-level network using a short-range radio, which is referred to as the original network. In NTM, we assume (a) that there is a trusted authority that is responsible for generating and launching mobile nodes, and (b) that mobile nodes are resilient against the unauthorized analysis and modification of their computation logic. 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 (Fig-1). *Node Initiator(NI)* is an authority responsible for generating and launching TMs into the network. It may be a piece of software, a node, or an organization, and it could be either inside or outside the network. In NTM, we assume that there is only one NI that is always-existing and trusted by every node. The NI launches one TM each time in a broadcast fashion into the backbone network. Before launching a TM, the NI associates it with a symmetric secret key, SK, and a monotonically increased version number (starting from 1). For this purpose, we adopt the formal Proofs of Cryptographic Security of Diffie-Hellman-based Protocols[25], [3]. The purpose of SK is to secure trust aggregation and reputation propagation, while the version number is used to support agent consistency verification. In case the SK of the current TM is stolen or broken, the NI may periodically launch a new TM with a higher version number and a fresh SK to replace old ones according to application-specific security requirements. *Trust Monitor(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 and reputation 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. HB accommodates n_i's TE last issued by $TM(n_i)$. As for COUNTR, it is incremented whenever $TM(n_i)$ receives

TABLE III
A TABLE OF TETBL OF NODE n_i

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

a message from a node for the first time since the last COUNTR resetting.

As illustrated in table III, 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, and its default value is 1. 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 Evaluator(TE)* 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:

$$TI(n_i, n_j, CNTXT) = EVAL_{SK}(D) \tag{5}$$

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.

IV. PROOF OF CORRECTNESS IN NTM MODEL

A trust management scheme, starts with a set of trust values, *D*. On top of that, we are likely to have ways to compare and combine elements of *D* which comprehends a given set of trust values (0, 1). Therefore, we have the trust definition in NTM as -

Definition 1: For any nodes in NTM, n_i and n_j, T_{n_i,n_j} denotes the trust measure for node n_j to handle(receive or forward) a packet from node n_i. $T_{n_i,n_j} \in (0, 1)$, where 0 means 'Untrustworthy' or 'no-trust' and 1 means a 'total trust' or 'trust-in-full'.

MANET decision-making does not end with providing the network with its initial organization. Deciding whether or not to forward a packet and even deciding which packet to drop might require different policies in different contexts. Therefore the following definition depicts the decision making mechanism under the influence of context based trust policy. Here a Markov policy [15] is a description of behaviours, which specifies the action to be taken in correspondence to each system state and time step.

Definition 2: A node in NTM, n_i, deciding the trust and taking an action to packet from another NTM node, n_j, can form a Markov decision process (MDP)[15]. For packet transportation from node n_i to node n_j, the recipient node, n_j can form a binary hypothesis testing based on certain decision policy. Trusted routing[16] therefore becomes a kind of Markov decision process where a decision/policy associated with a state-space. MDP[15] can be explained as $\langle S, A, Pr, R\rangle$

where *S* is the finit set of states, *A* denotes action set, $Pr(s, a, s')$ represents he probabilitywith which *s'* is reached when an action *a* is taken at state *s*. Now, for any node, n_i, knows its own Trust-Info but does not aware of other nodes in the network. Therefore, node n_i, has a finiteset of enquiring actions, a_i. When an action is taken, it results in some binary outcome $o \in O$. At each point in time, the node n_i, has a belief state over possible types of its counterpart, say, n_j. This relationship can be stated as - $b^{n_i}_{n_j}$.

Hence, the MDP proceeds in stages as:

At each time step, T, at which n_i has its current beliefs for n_j, takes an action *a*, observes the outcome *o* with a probability as:

$$P_{ni}(a, b^{n_i}_{n_j}) = \int_1^{-1} P(a_i|b_{n_i}) \int P(o|a_i) \left[r_{ni} + \gamma D(b^{o,a}_{n_i})\right] \tag{6}$$

where r_{ni} is the reward for n_i, D denotes the Trust value of being at the belief-state b_{ni} and $\gamma \in [-i, i]$ is the discount factor.

Lemma 1: Trust in NTM is *transitive*. That is, for $N = n_1, n_2, n_3, ..., n_i$ where $i \succ 0$ and n_i = N = nodes in NTM. Now, iff node n_i trusts node n_j and node n_j trusts n_k then n_i trusts n_k.

Lemma 2: Trust in NTM scheme is *irretrievable*. That is $T_{n_i,n_j} \neq T_{n_j,n_i}$.

Lemma 3: *Every node in NTM will eventually hold a copy of the latest TM.*

Proof. During the network initialization(NI) phase it broadcasts a TM in the backbone network, and it is guaranteed that all living backbone nodes receive the TE since the backbone network is connected despite backbone-node failure (by assumption). Therefore, every cluster head (that is a backbone node) broadcasts the received TE within its own cluster in the original network, but cluster members' receipt of the TE can not be guaranteed due to node failure or cluster re-organization. Under these circumstances, after the network initialization phase, all living backbone nodes hold a copy of the most-recently launched TM . Hence, every node in NTM will hold a copy of the latest TM and **Lemma 3** holds its correctness.

Theorem 1: *A node's reputation computed in NTM reflects*

the overall trust evaluation(TE) of other nodes on the node.
Proof. In NTM, by choosing the accurate reputation model, the computed reputation can accurately reflect nodes trustworthiness in a global view if sufficient individual trust evaluations of the node are provided. According to **Lemma 3**, for any node n_i, it holds all its TEs issued by other nodes. Therefore, the reputation computed by TM_{n_i} using this full set of TE will truly indicate the overall trust evaluation of ni from the other nodes' point of view. Hence, **Theorem 1** is correct.

Theorem 2: A node's locally-stored trusts are available to all the copies TMs but are confidential to any node including the node itself.

Proof. When a copy TM generates a TE, it encrypts the TE with its secret key SK. By Lemma 2, all the copies of TMs are eventually derived from the same original TM and share the same SK, and thus they are sooner or later able to successfully decrypt TEs generated by each other. Since SK is securely kept only by the copies of TMs, nodes are unable to reach TEs or received ones. Hence, **Theorem 2** holds.

V. Analysis and Discussion

The execution of NTM involves two phases; network formatting phase and the Trust Management interaction routine phase. As soon as NTM starts, the network formatting phase is initiated. The purpose of this phase is to distribute a TM to every node. What follows is the trust management interaction routine phase during which the trust and reputation service is provided. The following subsections depict the details of these two phases.

A. Network Formatting

The network formatting phase consists of two stages. In the first stage, the NI launches a TM in the network in a broadcast fashion. Considering an arbitrary node, n_i in the backbone network, when it receives a TM for the first time, n_i makes a copy of the TM and then forwards the TM to all its immediate neighbours in the backbone network. If n_i receives an already-received TM, it just discards the TM. Once n_i has a copy TM, it enters the second stage. In the second stage, n_i checks whether it is a cluster head itself. If so, n_i broadcasts its copy TM within its cluster in order to distribute the copy TM to all its cluster members, otherwise it keeps silent.

B. Trust Management interaction routine

As long as a node has a local copy TM, the trust and reputation service provided by the copy TM is available to the node, and thus we say that the node is in the service-offering phase. The trust and reputation service is composed mainly of two types of sub-services:
Trust value acquisition and *Trust management service routine*. The first sub-service is transaction-driven and involves the message transmission between the requester and provider, whereas the other sub-service involves merely the

Algorithm -1 (Trust value acquisition)

1. Node n_i sends a REQ-TRUST-VALUE to n_j
2. No-Reply-Transaction
   a. Sends a Request to the destination node
   b. Wait for Reply at given period of the $T_{TIMSTMP}$
   c. Sends Re-Request
   d. If No-Reply Absent Node
3. With-Reply-Transaction
   a. Sends a Request to the destination node
   b. Wait for Reply at given period of the $T_{TIMSTMP}$
   c. Get Reply
   d. TM validates the TRUST-VALUE by following the steps as
      i. Decrypt the TRUST-VALUE and Retrieve the TE
      ii. Compute TE by $EVAL_{SK}=f(\Phi,\Omega)$...equation (2)
4. If validity check is passed, then TM computes the trust of n_j based on the trust evaluation function
5. Otherwise, it considers that the TRUST-VALUE has been illegally modified.

Fig. 2. An Algorithm for Trust Value Acquisition

local processing periodically performed by the copy TM of each node. Because of the asynchronous execution, nodes are unlikely to enter the Trust management interaction routine phase at the same time. The trust value acquisition service consists of three algorithms to follow illustrated in fig-2, 3, 4 (Algorithm-1, 2, 3 respectively). Algorithm 1 depicts that a node n_i, in the network, requests TRUST-VALUEs from another node n_j. If ni does not get any response from n_j in a given period of time (TTMSTMP), then n_i re-sends the request to the same destination (n_j). If n_j does not reply for the second time, then it is (n_j) discarded by node n_i. Otherwise, with a given reply by n_j within given time period, TM of n_i then validates the TRUST-VALUE by decrypting it and then retrieve TE by equation 2. When the validity checks runs successfully, then TM of n_i computes the trust of n_j based on previously-run trust evaluation function. If the validity checks fails, then the TRUST-VALUE is being treated as 'illegally modified value'. Now, according to Algorithm 2, the transmission delay between each message transaction can be computed by deducting the timestamps between message transmission and message reception. It takes into account some relative delays and average delays as well. Finally, in algorithm 3, the pseudo-code reveals that for each and every trust evolution, there exists a trusted route to propagate TEs to the trusted nodes in NTM. All verifications and validations are conducted by using the time-stamp to keep track of the history of interactions. At the end of any successful interaction, it (e.g. node n_i) sends ACK = 1 to the destination node to terminate the session.
In NTM, we classify 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.

It should be noted that the transmission power of the nodes, which directly influences the number of TM nodes, has been chosen to a transmission range of certain distances(in meters). The transmission range decreases due to the consideration of the ground in the radio propagation

Algorithm – 2 (Computation of Transmission Delay)

1. Node n_i receives t_{ij} from n_j.
2. Compute
   a. $Relative\_delay_{TSTMP} = delay_{TSTMP} - average\_delay_{TSTMP}$
   b. $average\_delay_{TSTMP+1} = (1\text{-}w) \times average\_delay_{TSTMP} + delay_{TSTMP}$
   c. $delay_{TSTMP} = Recieve_{TSTMP} - Send_{TSTMP}$

Where w is the weight.

Fig. 3. An Algorithm for Computation of Transmission Delay

Algorithm – 3 Trust Propagation and Termination of *TM*

1. For every trust evolution, *TE (ID(n_i), CONTXT, t_{ij}, T)* submitted by node n_i from node n_j.
2. Find *ROUTE REQUEST(RTREQ)* and *ROUTE REPLY(RTREP)* to propagate *TE* to the trusted nodes in *NTM*.
3. *TM* verifies the validity of each node by $TI(n_i, n_j, CNTXT) = EVAL_{SK}(D)$
4. If $TI(n_i, n_j, CNTXT)$ is invalid then it is discarded by *TM*.
5. Else *TM* first retrieves the timestamp *T* from $TI(n_i, n_j, CNTXT)$ Then sends an $ACK = 1$ to the destination node.

Fig. 4. An Algorithm for Trust Propagation and Termination of TM

model with an increasing distance *d* m. The distribution time is measured as the time period between the initial sending and the earliest time at which all TM nodes have received the information.

VI. Conclusions

The goal of this paper was to provide a simple node-based trust management scheme for MANET with multiple perspectives on the concept of trust, an understanding of the properties, which should be considered in developing a trust metric, and insights on how a trust metric can be customized to meet the requirements and goals of the NTM scheme. The model is simple, flexible and easy to be implemented. After introducing and analysing the concept of node-based trust in MANET, we suggested future research directions to develop trust management schemes with desirable attributes such as adaptation to environmental dynamics, scalability and reliability. The proposed model will be simulated to gain further insight.

References

[1] A. Abdul-Rahman, S. Hailes, *Supporting trust in virtual communities*, In Proc. 33rd Ann. Hawaii Int'l Conf. Syst. Sci. (HICSS 33), vol. 6, (2000) pp. 6007-6016.

[2] A. Rahman and S. Hailes. *A Distributed Trust Model*. New Security Paradigms Workshop 1997. ACM, 1997.

[3] A. Roy, A. Datta, and J. C. Mitchell. *Formal proofs of cryptographic security of Diffie-Hellman-based protocols*. Manuscript, 2007. http://www.stanford.edu/arnab/rdm-DHProofs.pdf.

[4] C. Davis. *A localized trust management scheme for ad hoc networks*. Proceedings of 3rd International Conference on Networking (ICN'04). Mar. 2004.

[5] David B. Johnson. *Routing in Ad Hoc Networks of Mobile Hosts*. In Proceedings of the Workshop on Mobile Computing Systems and Applications, pp. 158-163, IEEE Computer Society, Santa Cruz, CA, December 1994.

[6] D. Johnson and D. Maltz. *Dynamic Source Routing in Ad Hoc Wireless Networks*, Mobile Computing, T. Imielinski and H. Korth, Ed., Kluwer, 1996.

[7] D. Balfanz, D. Smetters, P. Stewart and H. Wong. *Talking to Strangers: Authentication in Ad-hoc Wireless Networks*. NDSS. San Diego, 2002.

[8] H. Li and M. Singhal, *Trust Management in Distributed Systems*, Computers vol. 40, no.2, Feb. 2007, pp. 45-53.

[9] J. Liu, V. Issarny, *Enhanced reputation mechanism for mobile ad hoc networks*, In Proceedings of the Second International Conference on Trust Management, vol. 2995, Mar. 2004, pp. 48-62.

[10] 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.

[11] L.Eschenauer, V.Gligor and J. Baras. *On Trust Establishment in Mobile Ad-Hoc Networks*,Proceedings of 10th International Workshop of Security Protocols, Springer Lecture Notes in Computer Science (LNCS), Apr. 2002.

[12] L. Zhou and Z.J. Haas. *Securing ad hoc networks*. IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, November 1999.

[13] M. Gupta, P. Judge, M. Ammar, *A Reputation System for Peer-to-peer networks*, In Proc. 13th Int'l Workshop Netw. Oper. Syst. Support for Digital Audio and Video, Monterey, US, June 2003, pp.144-152.

[14] M. Virendra and S. Upadhyaya. *Securing Information through Trust Management in Wireless Networks*. Workshop on Secure Knowledge Management (SKM 2004). Buffalo, NY, 2004.

[15] R. Bellman. *A Markovian Decision Process*. Journal of Mathematics and Mechanics 6, 1957.

[16] R. Ferdous, V. Muthukkumarasamy, A. Sattar, *Trust Formalization in Mobile Ad-Hoc Networks*, Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications Workshops (AINA 2010), April 2010, Perth, Australia, pp. 351- 356

[17] R. Ferdous, V. Muthukkumarasamy, 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. (to appear)

[18] R. Jurca, B. Faltings. *An incentive compatible reputation mechanism*, In Proc. IEEE Int'l Conf. E-Commerce, June 2003.

[19] S. Buchegger, J.L. Boudec, *Nodes bearing grudges: towards routing security, fairness, and robustness in mobile ad hoc networks*, In Proc. Tenth Euromicro Workshop Parallel, Distr. Netw.-based Process., 2002, pp. 403-410.

[20] S. Buchegger, J. Boudec, *A robust reputation system for P2P and mobile ad-hoc networks*, In Proc. Second Workshop the Economics of Peer-to-Peer Systems, Cambridge, US, June 2004.

[21] S.D. Kamvar, M.T. Schlosser, H. Garcia-Molina. *The Eigentrust algorithm for reputation management in P2P networks*, In Proc. 12th Int'l World Wide Web Conf., Budapest, Hungary, 2003, pp. 640-651.

[22] 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.

[23] T. Beth, M. Borcherding and B. Klein. *Valuation of trust in open networks*. Proceedings of ESORICS 1994, November 1994.

[24] T. Hughes, J. Denny, P. Muckelbauer, J. Etzl. *Dynamic Trust Applied to Ad Hoc Network Resources*.Autonomous Agents and Multi-Agent Systems Conference, Melbourne, Australia, 2003.

[25] W. Diffie and M. E. Hellman. *New directions in cryptography. IEEE Transactions on Information Theory*, IT-22(6):644654, 1976.

[26] Y. Huang and W. Lee. *A Cooperative Intrusion Detection System for Ad Hoc Networks*. Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03). Fairfax VA, October 2003.

[27] Y. Wang, J. Vassileva, *Trust and reputation model in peer-to-peer networks*, In Proc. Third Int'l Conf. Peer-to-Peer Comput. (P2P'03), Linkoping, Sweden, Sep. 2003, pp. 150-157.