www.ijiarec.com

ISSN: 2348-2079

MAR-2015

International Journal of Intellectual Advancements and Research in Engineering Computations

SECURITY ENHANCEMENT FOR EFFICIENT ROUTING IN MANET

[1]R.Arthi, [2]E.Padma, [3]Dr.N.Shanthi

ABSTRACT

Mobile ad hoc networks (MANETs) are a dynamic network in which the mobile node does not have any infrastructure. Link breakages exist due to its high mobility of nodes which leads to frequent path failures and route discoveries. The neighbor coverage and probabilistic mechanism significantly decreases the number of retransmissions so as to reduce the routing overhead. Since security is also a challenging factor in adhoc networks a concept of secured efficient routing is included with NCPR which enables a new trust approach based on the extent of friendship between the nodes is proposed which makes the nodes to co-operate and prevent flooding attacks in an ad hoc environment. All the nodes in an ad hoc network are categorized as friends, acquaintances or strangers based on their relationships with their neighboring nodes. During network initiation all nodes will be strangers to each other. A trust estimator is used in each node to evaluate the trust level of its neighboring nodes. This approach combines the advantages of the neighbor coverage knowledge and the probabilistic mechanism, which can significantly decrease the number of retransmissions so as to reduce the routing overhead, and improve the security. Specifically, throughput and packet delivery ratio can be improved significantly.

Keywords - Bandwidth-constrained, security, Unicasting, Multicasting.

INTRODUCTION

With recent advances in wireless technologies and mobile devices, Mobile Ad hoc Networks (MANETs) [1], [2] have become popular as a key communication technology in military tactical environments such as establishment of communication networks used to coordinate military deployment among the soldiers, vehicles, and operational command centers [3]. There are many risks in military environments needed to be considered seriously due to the distinctive features of MANETs, including open wireless transmission medium, nomadic and distributed nature, lack of centralized infrastructure of security protection [4]–[6]. Therefore, secured routing in tactical MANETs is a challenging research topic

There are two complementary classes of approaches that can safeguard tactical MANETs: prevention-based and detection- based approaches [8]. Prevention-based approaches are studied comprehensively in MANETs [9]–[12]. One issue of these prevention-based approaches is that a centralized key management infrastructure is needed, which may not be realistic in distributed networks such as MANETs. In MANETs, this is especially true given the low secured routing between mobile devices [14], [15]. Serving as the second wall of protection, detection-based approaches can effectively help identify malicious activities [16]–[18].

Although some excellent work has been done on detection-based approaches based on trust in MANETs, most of existing approaches do not exploit direct and indirect observation (also called secondhand information that is obtained from third party nodes) at the same time to evaluate the trust of an observed node. Moreover, indirect observation in most approaches is only used to assess the reliability of nodes, which are not in the range of the observer node [19] Therefore, inaccurate trust values may be derived. In

Author for Correspondence:

[1]PG Scholar (CSE), Nandha Engineering College, Erode, Tamilnadu, India. Email: adjomn@gmail.com.

[2]Assistant Professor (CSE), Nandha Engineering College, Erode, Tamilnadu, India. Email:padmasents@gmail.com.

[3]Professor and Dean (CSE), Nandha Engineering College, Erode, Tamilnadu, India. Email: shanthi.moorthi@gmail.com.

addition, most methods of trust evaluation from direct observation [19], [20] do not differentiate data packets and control packets. However, in MANETs, control packets usually are more important than data packets.

In this paper, we interpret trust as the degree of belief that a node performs as expected. We also recognize un- certainty in trust evaluation. Based on this interpretation, we propose a trust management scheme to enhance the security of MANETs. The difference between our scheme and existing schemes is that we use uncertain reasoning to derive trust values. Uncertain reasoning was initially proposed from the artificial intelligence community to solve the problems in expert systems, which have frequent counter-factual results . The elasticity and flexibility of uncertain reasoning make it successful in many fields, such as expert systems, multi- agent systems, and data fusion. The contributions of this paper are outlined as follows:

We propose a unified trust management scheme that enhances the security in MANETs using uncertain reasoning. In the proposed scheme, the trust model has two components: trust from direct observation and trust from indirect observation. With direct observation from an observer node, the trust value is derived using Bayesian inference, which is a type of uncertain reasoning when the full probability model can be defined. On the other hand, with indirect observation from neighbor nodes of the observer node, the trust value is derived using the Dempster-Shafer theory, which is another type of uncertain reasoning when the proposition of interest can be derived by an indirect method.

The proposed scheme differentiates data packets and control packets, and meanwhile excludes the other causes that result in dropping packets, such as unreliable wireless connections and buffer overflows.

We evaluate the proposed scheme in a MANET routing protocol, the Neighbor coverage probabilistic rebroadcast protocol, with the NS2 simulator. Extensive simulation results show the effectiveness of the proposed scheme. Throughput and packet delivery ratio can be improved significantly, with slightly increased average end-to-end delay and overhead of messages.

The remainder of this paper is organized as follows. The trust model and its two components are presented in Section II. Section III depicts the secure routing based on trust with direct observation and indirect observation. Section IV describes the performance and effectiveness of our scheme. Finally, we conclude the work in Section V.

TRUST MODEL IN MANET

In this section, we describe the definition and properties of trust in MANETs. Based on the definition, we depict the trust model that is used to formulate the trust between two nodes in MANETs, and present a framework of the proposed scheme. The main notations that are used in this paper are summarized in Table I.

DEFINITION AND PROPERTIES OF TRUST

Trust has different meanings in different disciplines from psychology to economy [17]. The definition of trust in MANETs is similar to the explanation in sociology, where trust is interpreted as degrees of the belief that a node in a network nodes may have different trust values of the same observed node. Dynamicity means that the trust of a node should be changed depending on its behaviors. Non-transitivity means that if node A trusts node B and node B trusts node C, then node A does not necessarily trust node C. Asymmetry means that if node A trusts node B, then node B does not necessarily trust node A.

TABLE I

MAIN NOTATIONS

NOTATION	DEFINITION
T_{AB}	The trust value that node A give node B
T^{S}_{AB}	The trust value that node A gives node B based on direct observation of Node A
T^{N}_{AB}	The trust value that node A gives node B based on indirect observation of node A

T^{D}_{AB}	The trust value that node A gives node B based on data packets
T^{C}_{AB}	The trust value that node A gives node B based on control packets
Λ	The weight for the trust value based on direct observation
P	The weight for the trust value based on data packets
Γ	Punishment factor ≤ 1

Context-dependency means that trust assessment commonly bases on the behaviors of a node. Different aspects of actions can be evaluated by different trust. For example, if a node has less power, then it may not be able to forward messages to its neighbors. In this situation, the trust of power in this node will decline, but the trust of security in this node will not be changed due to its state. Reputation is another important concept in trust evaluation. Reputation reflects the public opinions from members in a community. In MANETs, reputation can be a collection of trust from nodes in the network. Reputation is more global than trust from the perspective of the whole network .

TRUST MODEL

.

Based on the definition and properties of trust in MANETs, we evaluate trust in the proposed scheme by a real number, T , with a continuous value between 0 and 1. Although trust and trustworthiness may be different in contexts, in which the trust or needs to consider risk [18], trust and trustworthiness are treated the same for simplicity in the proposed scheme.

In this model, trust is made up of two components: direct observation trust and indirect observation trust. These components are similar to those used in . In direction observation trust, an observer estimates the trust of his one-hop neighbor based on its own opinion. Therefore, the trust value is the expectation of a subjective probability that a trust or uses to decide whether or not a trustee is reliable. It is similar to first-hand information defined by [19], [20].We denote T^{S} as a trust value from direct observation and can be calculated by Bayesian inference. If we only consider direct observation, there would be prejudice in trust value calculation. In order to obtain less biased trust value, we also consider other observers' opinions in this paper. Although opinions of neighbors are introduced in , the method that simply takes arithmetic mean of all trust values is not sufficient to reflect the real meaning of other unreliable observers' opinions because there are two situations that may severely disturb the effective evidence from neighbors: unreliable neighbors and unreliable observation [19]. Unreliable neighbors themselves are suspects. Even though neighbors are trustworthy, they may also provide unreliable evidence due to observation conditions. The Dempster-Shafer theory is a good candidate to aid in this situation, in which evidence is collected from neighbors that may be unreliable. Therefore, We denote the trust value derived from indirect observation.

$$T = \lambda T^{S} + (1 - \lambda)T^{N} , \qquad (1)$$

where λ is a weight assigned to T^{S} , $0 \le \lambda \le 1$.

FRAMEWORK OF THE PROPOSED SCHEME

Based on the trust model, the framework of the proposed scheme is shown in Fig. 1. In the trust scheme component, the module of trust evaluation and update can obtain evidence from direct and indirect observation modules and then utilize two approaches, Bayesian inference and DST, to calculate and update the trust values. Next, the trust values are stored in the module of trust repository. Routing schemes in the networking component can establish secure routing paths between sources and destinations based on the trust repository module. The application component can send data through secure routing paths.

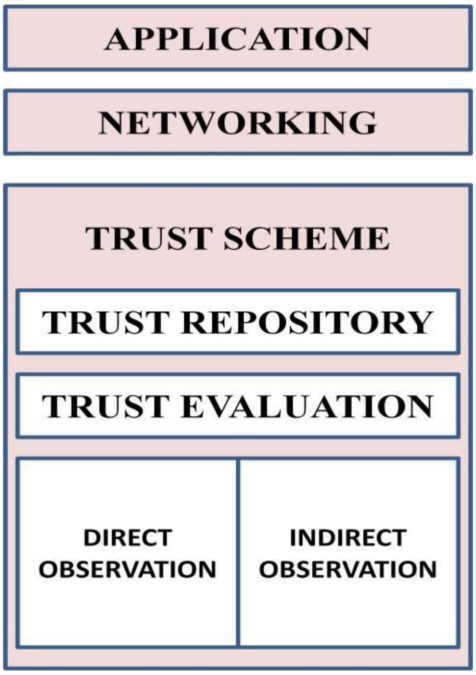


Fig 1. The Framework of the proposed scheme

The trust from direct observation between an observer node A and an observed node B in this trust scheme can be defined further as

$$T^{S}_{AB} = \rho T^{D}_{AB} + (1-\rho)T_{AB} , \qquad (2)$$

Where $\rho (0 \leq \rho \leq 1)$ is the weight of the data packet. T^{C}_{AB} is the trust value based on the control packets.

SECURE ROUTING BASED ON TRUST

The original NCPR does not provide security measurements in the protocol. NCPR assumes that every node are cooperative.This assumption is inappropriate in military environment. Modification of NCPR include the following :route selection based on link metrics and trust value calculation Link metrics information can be added to message as Type Length Value(TLV)blocks.

Algorithm 1 depicts the details of each iteration. Algorithm2 describes that an observer node collects evidence from its one-hops neighbors

between the observer node and the observed node. After T^{S} and T^{N} are obtained, we can get the total trust value of the observed node by (1). In proactive routing protocols, such as NCPR, an observer node can obtain the information from its neighbor nodes periodically by control messages

Compared to the existing NCPR scheme that uses the shortest path based on hop count, we derive the best routing path considering both trust values and hop count. We use the Dijkstra' algorithm to calculate the best routing path. Since minimization is used in the Dijkstra' algorithm we need to convert the trust value to untrustworthy value..

The trust values and routing table of each node can be stored in the Trust Platform Module (TPM), which provides additional security protection in open environments with the combination of software and hardware. Since the trust values in each node are the key facilities to detect malicious nodes, the TPM is able to provide effective protection to secure routing to avoid malicious attacks by enemies in battlefields.

Algorithm 1 Trust Calculation with Direct Observation

```
if node A, which is an observer, finds that its
one-hop neighbor, Node B that is a trustee,
receives a packet then
    the number of packets received increases one
    if node A finds that node B forwards the
    packet successfully then
        the number of packets forwarded increases one
    else
        if TTL of the packet becomes zero or
        overflow of buffers in node B or the state
        of wireless connection of node B is bad
        then
            the number of packets received decreases one
        end if
    end if
end if
calculate the trust value, $T^S$
```

Algorithm 2 Trust calculation with Indirect Observation

```
if node A which is an observer which has more
    than one hop neighbors between it and the trustee,
    node B then
  calculates the trust value, $T^N$
else
  set $T^N$ to 0
  set $\lambda$ to 1
end if
```

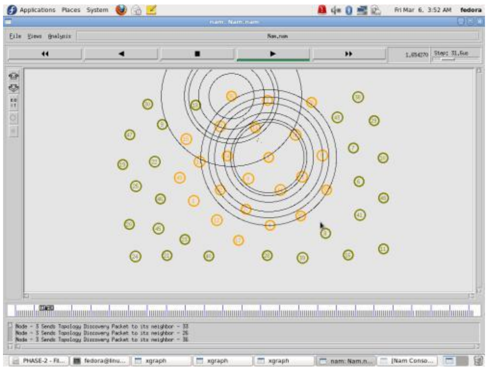
SIMULATION RESULT AND DISCUSSIONS

The proposed system is simulated on the NS2 platform with NCPR protocol .In the simulations the effectiveness of the scheme is evaluated in an insecure environment.

ENVIRONMENT SETTING

Nodes are placed randomly in the defined area. Each scenario has a pair of nodes as the source and destination with Constant Bit Rate. The simulation parameters are listed in Table II. In our simulations, we assume that there are two types of nodes in the network: normal nodes, which follow the routing rules, and compromised nodes, which drop or modify packets maliciously. We also assume that the number of compromised nodes is minor compared to the total number of nodes in the network.

There are three performance metrics considered in the simulations: 1) *Packet delivery ratio (PDR)* is the ratio of the number of data packets received by a destination node and the number of data packets generated by a source node; 2) *Throughput* is the total size of data packets correctly received by a destination node every second; 3) *Message Overhead* is the size of Type Length Value (TLV) blocks in total messages, which are used to carry trust values;



```
Node - 3 Sends Topology Discovery Packet to its neighbor - 33
Node - 3 Sends Topology Discovery Packet to its neighbor - 26
Node - 3 Sends Topology Discovery Packet to its neighbor - 36
```

Fig 2.An example of network setup

TABLE II

SIMULATION PARAMETER

PARAMETER	VALUE
Application Protocol	CBR
Packet size	512 bytes
Routing Protocol	NCPR
Data rate	2Mbps
Simulation area	200mx200m
Number of nodes	0-49
Simulation time	300s

The simulation parameters are listed in Table II. There are two types of nodes involved in simulation: normal nodes that follow routing routes, and compromised nodes ,which drop or modify packets maliciously.

A. PERFORMANCE IMPROVEMENT

The NCPR protocol with trust management is evaluated in the simulation,

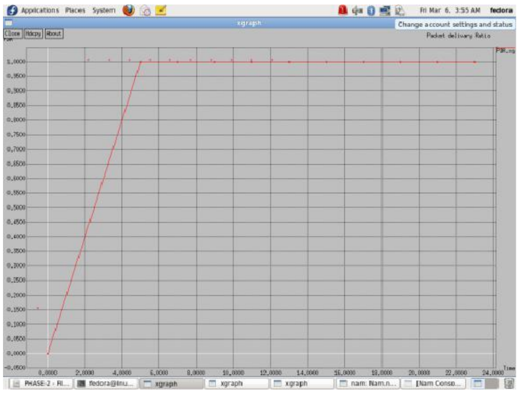


Fig 2.Packet Delivery Ratio versus the number of nodes in the network

In Fig 2,we can see the proposed system packet delivery ratio with trust based routing calculation.

When the number of malicious nodes increases there will be drop in throughput. compared to the proposed scheme the existing scheme has a very low throughput even if the number of malicious node is small.

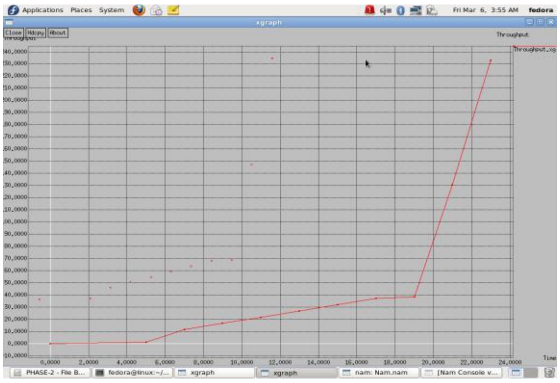


Fig 3.Throughput versus the number of nodes in the network

In Fig 3. throughput increases gradually. This is because the higher speed of a node may increase the probability of packets lost .Packet drop remains constant in Fig 4

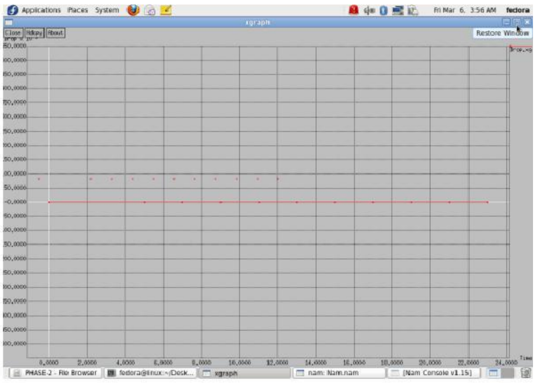


Fig 4 Packet drop versus number of nodes

B. COST

The cost of security enhancement in NCPR mainly includes the increased average end-to-end delay and overhead of messages that are used to carry trust values of nodes. Because trust values are embedded in the HELLO messages and TC messages, there is no more messages need to be sent. The overhead is not very high. This is because, when the number of nodes increases, the total message becomes large. Then the 12-byte overhead is trivial compared to the size of messages As the number of nodes increases, the routing load of the existing and proposed schemes climb up due to the nature of proactive routing protocol: periodical generation of control messages in every node.

CONCLUSION AND FUTURE WORK

In this paper, we proposed a unified trust management scheme that enhances the security of MANETs. Using recent advances in uncertain reasoning, Bayesian inference and Dempster-Shafer theory, we evaluate the trust values of ob- served nodes in MANETs. Misbehaviors such as dropping or modifying packets can be detected in our scheme through trust values by direct and indirect observation. Nodes with low trust values will be excluded by the routing algorithm. Therefore, secure routing path can be established in malicious environments. Based on the proposed scheme, more accurate trust can be obtained by considering different types of packets, indirect observation from one-hop neighbors and other important factors such as buffers of queues and states of wireless connections, which may cause dropping packets in friendly nodes. The results of MANET routing scenario positively support the effectiveness and performance of our scheme, which improves throughput and packet delivery ratio considerably, with slightly increased average end-to-end delay and overhead of messages. In our future work, we will extend the proposed scheme to MANETs with cognitive radios

REFERENCES

[1] S. Corson and J. Macker, "Mobile ad hoc networking (MANET): routing protocol performance issues and evaluation considerations," IETF RFC 2501.JAN 1999

[2] F. R. Yu, Cognitive Radio Mobile Ad Hoc Networks. New York: Springer, 2011.

[3] J. Loo, J. Lloret, and J. H. Ortiz, Mobile Ad Hoc Networks: Current Status and Future Trends. CRC Press, 2011.

[4] Q. Guan, F. R. Yu, S. Jiang, and V. Leung, "Joint topology control and authentication design in mobile ad hoc networks with cooperative communications," IEEE Trans. Veh. Tech., vol. 61, pp. 2674 – 2685, July2012

[5] F. R. Yu, H. Tang, S. Bu, and D. Zheng, "Security and quality of service (QoS) co-design in cooperative mobile ad hoc networks," EURASIP J. Wireless Commun. Networking, vol. 2013, pp. 188–190, July 2013

[6] Y. Wang, F. R. Yu, H. Tang, and M. Huang, "A mean field game theoretic approach for security enhancements in mobile ad hoc networks," IEEE Trans. Wireless Commun., vol. 13, pp. 1616–1627, March 2014.

[7] J. Chapin and V. W. Chan, "The next 10 years of DoD wireless networking research," in Proc. IEEE Milcom'11, (Baltimore, MD, USA), Nov. 2011.

[8] S. Bu, F. R. Yu, P. Liu, P. Manson, and H. Tang, "Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks," IEEE Trans. Veh. Tech., vol. 60, pp. 1025-1036.Mar.2011

[9] C. Adjih, D. Raffo, and P. Muhlethaler, "Attacks against OLSR: dis- tributed key management for security," in Proc. 2nd OLSR Workshop, (Domaine de Voluceau, France), Dec. 2005.

[10] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," IEEE Trans. Dependable andSecure Computing, vol. 3, pp. 386–399, Oct.–Dec. 2006.

[11] Y. Fang, X. Zhu, and Y. Zhang, "Securing resource-constrained wireless ad hoc networks," IEEE Wireless Comm., vol. 16, no. 2, pp. 24–30, 2009.

[12] F. R. Yu, H. Tang, P. Mason, and F. Wang, "A hierarchical identity based key management scheme in tactical mobile ad hoc networks, "IEEE Trans. on Network and Service Management, vol. 7, pp. 258 – 267.Dec 2010.

[13] S.Marti, T. Giuli, K. Lai, and M. Maker, "Mitigating routing mis-behavior in mobile ad hoc networks," in Proc. ACM MobiCom'00, (New York, NY, USA), Aug. 2000.

[14] W. Lou, W. Liu, Y. Zhang, and Y. Fang, "SPREAD: improving network security by multipath routing in mobile ad hoc networks," ACM Wireless Networks, vol. 15, no. 3, pp. 279–294, Mar. 2009

[15] R. Zhang, Y. Zhang, and Y. Fang, "AOS: An anonymous overlay system for mobile ad hoc networks," ACM Wireless Networks, vol. 17, no. 4, pp. 843–859, May 2011.

[16] P. Albers, O. Camp, J.-M. Percher, B. Jouga, and L. M. R. S. Puttini, "Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches," in Proc. 1st Int'l Workshop on Wireless information Systems, (Ciudad Real, Spain), Apr. 2002.

[17] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks," IEEE Wireless Comm., vol. 11, pp. 48–60, Feb. 2004.

[18] S. Bu, F. R. Yu, X. P. Liu, and H. Tang, "Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks," IEEE Trans. Wireless Commun., vol. 10, pp. 3064 – 3073, Sept. 2011.

[19] S. Buchegger and J.-Y. L. Boudec, “A robust reputation system for P2P and mobile ad-hoc networks,” in Proc. 2nd Workshop on the Economics of Peer-to-Peer Systems, (Bologna, Italy), Nov. 2004.

[20] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, “A quantita- tive trust establishment framework for reliable data packet delivery in

MANETs,” in Proc. 3rd ACM Workshop on SASN’05, (Alexandria, VA, USA), Nov. 2005.