IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-10, Oct 2018 E-ISSN: 2347-2693

Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning

R. Esther Raja Pushpa

Dept. of computer science, Dr.Sivanthi Aditanar college of Engineering, Tiruchendur, Tamilnadu, India.

Available online at: www.ijcseonline.org

Accepted: 19/Oct/2018, Published: 31/Oct/2018

***Abstract*—** The mobile ad hoc networks (MANETs) has a dynamic topology and open wireless medium, may leads to MANET suffering from many security liabilities. In this paper, using recent progresses in uncertain reasoning initiated from artificial intelligence community, an unified trust management scheme has been implemented that improves the security in MANETs. In the proposed trust management pattern, the trust model has two components: trust from direct observation and trust from indirect observation. In direct observation from an observer node, the trust value is derived using Bayesian inference, which is a form of uncertain reasoning. In Indirect observation, also called secondhand evidence that is obtained from neighbor nodes of the observer node, here the trust value is derived using the Dempster-Shafer theory, which is another form of uncertain reasoning. Merging these two components in the trust model can achieve more accurate trust values of the observed nodes in MANETs. Then evaluate this pattern under the situation of MANET routing protocol (OLSRv2). The simulation result shows the effectiveness of the proposed scheme. Exactly, throughput and packet delivery ratio can be improved considerably.

***Keywords*—** MANETs, Security, Trust Management, Uncertain Reasoning.

I. INTRODUCTION

Wireless Network:

Wireless Network is a type of computer network that uses wireless connections for linking network nodes.

Wireless Ad Hoc Network:

A wireless ad hoc network is not a centralized type of wireless network. The network of which nodes forward data is made dynamically on the basis of routing. Ad hoc networks can use flooding for forwarding packets.

Mobile Ad Hoc Network (MANET):

A mobile ad hoc network (MANET) is an endlessly self-organizing, infrastructure-less network of mobile nodes connected without wires. Each device in MANET is free to travel independently in any direction, therefore it will change its links to other devices regularly. The principal challenge in building a MANET is maintaining each device to continuously keep the information required to proper route traffic. Such networks may function by themselves or may be connected to a superior Internet. It contains one or multiple different transceivers between nodes. This results in highly active, and independent topology .MANETs is an type of Wireless ad hoc network that has a routable networking environment. MANET is a peer-to-peer, self-forming network of multiple nodes that has an essential controller to resolve, optimize, and issue the routing table.

MANET types:

Vehicular Ad Hoc Networks (VANETs) are used for communication among vehicles and between vehicles and wayside equipment. Smart vehicular ad hoc networks are a variety of artificial intelligence that helps vehicles to behave in sharp manners during accidents, drunken driving etc.

Smart Phone Ad Hoc Networks (SPANs) is the power of the existing hardware in commercially obtainable smart phones to create peer-to-peer networks without depending on cellular networks**.**

Internet based Mobile Ad Hoc Networks (iMANETs) are ad hoc networks that links mobile nodes and fixed nodes .In such type of networks usually have ad hoc routing algorithms but can’t able to apply openly.
Military / Tactical MANETs are used by military environment with importance of security and centralized controller.

MANET applications:

Mobile Ad hoc Networks (MANETs) have become fashionable as a key communication technology in military environments such as establishment of communication networks used to manage military consumption among the soldiers, vehicles, and operational centers. There are many risks in military environments needed to be considered critically due to the features of MANETs, including open wireless transmission medium, and lack of centralized infrastructure of security guard.

Approaches:

MANET can be separated into two classes: prevention based and detection based. One issue of these prevention-based approaches, there is a need for centralized key managing infrastructure which may not be sensible in distributed networks. In addition, a centralized infrastructure will be the main object of rivals in battlefields. If the infrastructure is impaired, then the whole network may also be destroyed. Although prevention-based approaches can avoid misbehavior nodes, there are still chances for accuring malicious nodes to participate in the routing system and disturb the routing process. Detection-based approaches can successfully help identify malicious activities. In this approach, the security has been enhanced based on trust in MANETs.

Security based on trust:
Trust is a relationship established between two entities for a specific action. In particular, one entity trusts the other entity to perform an *action*. In this work, the first entity is called the observer node, the second entity is called the observed node.

Trust evaluation based on Uncertainty:
Trust is the degree of belief that a node performs as expected. The importance of uncertainty in trust is a major issue. To enhance the security of MANETs, trust management scheme under uncertainty has been developed. Trust is a measure of uncertainty. Uncertainty means unpredictable or unavailable information. In particular, if the observer node believes that the observed node will perform the action for sure, then there is no uncertainty; if the observer node believes that the observed will not perform the action for sure, then there is some degree of uncertainty. If the observer node does not have any plan of whether the observed node will perform the action or not, that does not have trust in the observed node. In this case, the source has the peak uncertainty. The level of trust can be measured by a real number T, referred to as the trust value. Trust value should describe uncertainty. The observer may have different trust values with the similar observed node for the similar action. Trust properties are,

- Subjectivity- It means that an Observer node has a rights to decide the trust of an observed node.
- Dynamicity- It means that the trust of a node must be changed depending on its actions.
- Non-transitivity- It means that if a node A trusts node B and node B trusts node C, then node A does not need to trust node C.
- Asymmetry- It means that if node A trust node B, then node B does not necessarily trust node A.
  Trust method has two components:
  Direct observation
  Indirect observation.

Direct observation from an observer node, the trust value T^S is derived using Bayesian inference, which is a form of uncertain reasoning. Indirect observation from neighbor nodes of the observer node, the trust value T^N is derived using the Dempster-Shafer theory, which is another form of uncertain reasoning. Combining the trust value T^S, from direct observation and the trust value T^N, from indirect observation, Its can get a more realistic and accurate trust value(T) of a node in MANETs.

$$T = \lambda T^S + (1 - \lambda)T^N;$$

λ is a weight factor assigned to T^S , $0 \leq \lambda \leq 1$.

The proposed scheme has been implemented in MANET routing protocol, the optimized link state routing protocol version 2 (OLSRv2). OLSRv2 is a proactive routing protocol, which is a new version of OLSR. OLSRv2 inherits OLSR's core algorithms and also introduces some new features: routing Multipoint Relay (MPR), flexible link metrics, extensible message formats, etc**.**

II. Module Discription

1. Direct Observation
In the direct observation, each observer can watch the number of packets forwarded by an observed node and equate them with original packets so that the observer can identify the malicious activities of the observed node.

Therefore, the observer node can compute the trust values of its neighboring nodes by using Bayesian inference, which is a general framework to deduce the estimation of the unknown probability by using observation.

The degree of belief is a random variable, denoted by Θ and
$0 \leq \theta \leq 1$. From Bayes' theorem, we can derive the following formulation,

$$\mathbf{T^S} = \frac{\mathbf{p(x,y)f(y)}}{\mathbf{p(x,y)f(y)+p(x1,y)\ f(y)}},$$

$\mathrm{T^S}$- Trust value obtained by direct observation.

$p(x, y)$ - Probability value between the number of packets forwarded and received.

x - The number of packets forwarded by an observer node.

y - The number of packets received by an observed node.

$x1$ - The number of packets forwarded by an observed node.

It is the value of the number of packets received by an observed node divided by the number of packets forwarded by an observer node.

p(x,y)= y/x

It is the value of the number of packets forwarded by an observed node divided by the number of packets received by an observed node.

p(x1,y)=x1/y

$f(y)$ is obtained by the expectation of the Beta distribution,

f(y)=α/(α+β)

α ,β is a randam variables, α ,β >0.

Due to reproductivity of (4), the trust value is calculated iteratively. At the beginning, there is no observation. The prior distribution *f*(*y*) is *Beta* (*θ*; 1, 1) at the beginning. then,

$$f(y) = \frac{\alpha_n}{\alpha_n + \beta_n}$$

$$\alpha_n = \alpha_{n-1} + x_{n-1}$$

$$\beta_n = \beta_{n-1} + y_{n-1} - x_{n-1}$$

$$\alpha_0, \beta_0 = 1, n \in \mathbb{Z}^+.$$

Initially there is no data transmission will be performed.so that the trust value of a node is 0.5 at the beginning. That means the node is viewed as neutral when no history records are created. The value of trust can be revised continuously through complement observation.

```
Algorithm1: Trust Calculation with Direct Observation:
    Step1: 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
        Step2: if node A finds that node B forwards the packet successfully
            then the number of packets forwarded increases one
            else
    Step3: if  TTL of the packet becomes zero or overflow of buffers in node B or the State of wireless connection in node B
            then the number of packets received decreases one
            end if
        end if
    end if
    calculate the trust value, $T^S$,  and update the old one.
```

2. Indirect Observation

In indirect observation, the trust values from neighbouring nodes are collected and that are used to evaluate the trust value of the observed node will be discussed.

Collection of neighbours opinion can help in qualifying whether or not a node is aggressive. This mechanism may reduce the prejudice from an observer.

A situation in which a node is kind to one node but malicious to others may be eased. In order to implement this method, the Dempster-Shafer theory, which is a mathematical theory of proof, is used as it is well established for handling with uncertainty or ignorance, and it provides a mathematical measurement of degrees of belief about a intention from multiple sources .

The core of this theory is the belief function. The degrees of belief about a scheme can be obtained from subjective probabilities.

In the indirect observation, when the trust evaluation is performed with DST, assume that there are more than one nearby nodes between an observer and an observed node and also assume that the evidence provided by different neighbours is independent.

Based on the frame of judgment, the basic probability value of focal set A_i, is a function $m : 2^{\Omega} \rightarrow [0,1]$, which satisfies following conditions: $m(\theta) = 0$ and $\sum_{A_{i \in B}} m(A_i)$. For any subset B of the frame of discernment the belief function is defined as,

$$bel(B) = \sum_{A_i \subseteq B} m(A_i).$$

bel(B) is a belief function of node B on node A.

$A_i$is the neighbouring nodes of both A and B.

$m(A_i)$is trust value evaluation.

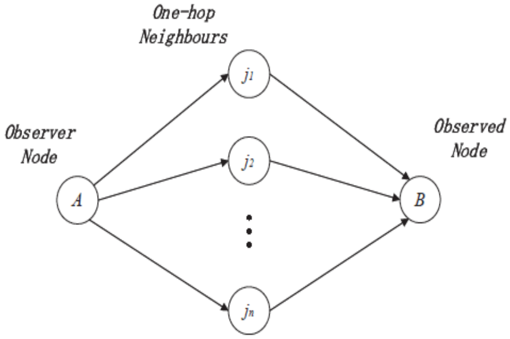


Figure 5.1 Trust evaluation

As like as the above figure 5.1, there are the number of nodes between node A and B. Here the two security states to a node, i.e., trustworthy, untrustworthy. Therefore, the frame of judgment in the Dempster-Shafer theory,

$$\Omega = \{trustworthy, untrustworthy\},$$

Which proves that node *B* has two states: trustworthy and untrustworthy. Node *A* estimates the trust value of node B through one-hop neighbors between them. One-hop neighbours of node *B* can provide evidence to a subset of Ω with hypothesis *H*, that is node *B* is trustworthy.

Hypothesis *H* = *{trustworthy}*;

Hypothesis $\overline{H}$= *{untrustworthy}*;

Hypothesis*U*= Ω, which means that the observed node *B* is either in the trustworthy state or untrustworthy state.

Each one-hop neighbours gives suggestion from its observation by assigning its beliefs. Each hypothesis is assigned a basic probability value *m*(*H*) between 0 and 1. In this scheme, the basic probability value can be achieved from direct observation. for example, the trust value of node *j*1 is T^{S}_{Aj1}, from direct observation of node *A* to node *j*1. If node *j*1 believes that node B is trustworthy, then the basic probability value m_{j1}(*H*) is T^{S}_{Aj1}, and $m_{j1}(\overline{H})$ is 0. From the definition of belief function, m_{j1}(*U*) is equal to 1 − T^{S}_{Aj1}.

$$
\begin{aligned}
m_{j_1}(H) &= T^{S}_{Aj_1},\\
m_{j_1}(\overline{H}) &= 0,\\
m_{j_1}(U) &= 1 - T^{S}_{Aj_1},
\end{aligned}
$$

If node *j*1 considers that node B is untrustworthy, the formulae are as follows:

$$
\begin{aligned}
m_{j_1}(H) &= 0,\\
m_{j_1}(\overline{H}) &= T^{S}_{Aj_1},\\
m_{j_1}(U) &= 1 - T^{S}_{Aj_1},
\end{aligned}
$$

In this scenario, assume that there are number of one-hop neighbours close to node *B* as shown in Fig. 5.1. Therefore, the combined belief of node *j*1 and node *j*2 is calculated as follows,

$$
\begin{aligned}
m_{j_1}(H) \oplus m_{j_2}(H) &= \frac{1}{K}[m_{j_1}(H)m_{j_2}(H)\\
&\quad + m_{j_1}(H)m_{j_2}(U)\\
&\quad + m_{j_1}(U)m_{j_2}(H)],\\
m_{j_1}(\overline{H}) \oplus m_{j_2}(\overline{H}) &= \frac{1}{K}[m_{j_1}(\overline{H})m_{j_2}(\overline{H})\\
&\quad + m_{j_1}(\overline{H})m_{j_2}(U)\\
&\quad + m_{j_1}(U)m_{j_2}(\overline{H})],\\
m_{j_1}(U) \oplus m_{j_2}(U) &= \frac{1}{K}m_{j_1}(U)m_{j_2}(U),
\end{aligned}
$$

Where,

$$
\begin{aligned}
K &= m_{j_1}(H)m_{j_2}(H) + m_{j_1}(H)m_{j_2}(U)\\
&\quad + m_{j_1}(U)m_{j_2}(U) + m_{j_1}(U)m_{j_2}(H)\\
&\quad + m_{j_1}(U)m_{j_2}(\overline{H}) + m_{j_1}(\overline{H})m_{j_2}(\overline{H})\\
&\quad + m_{j_1}(\overline{H})m_{j_2}(U).
\end{aligned}
$$

Under the rule of combination of belief, more results from neighbouring nodes are combined. Based on the Dempster-shafer theory, T^{N}_{AB} is defined as,

$$
T^{N}_{AB} = m_{j_1}(H) \oplus m_{j_2}(H) \ldots \oplus m_{j_n}(H),
$$

where node j_i, 1 ≤ i ≤ n, is an one-hop neighbor of node A and node B.

Algorithm 2: Trust Calculation with Indirect Observation:

```
Step1:  if node A, which is an observer, has more than one-hop neighbours between it and the trustee, node B
Step2:  then calculates the trust value, $T^{N}$ else,
Step3:  set $T^{N}$ to 0
        set $\lambda$ to 1
        end if
```

3. Trust Evaluation and Update:

Combining the trust value, T^{S}, from direct observation and the trust value, T^{N}, from indirect observation, the more precise and accurate trust value of a node has been obtained in MANETs.

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

where λ is a weight assigned to T^{S} , 0 ≤ λ ≤ 1.

4. Routing based on OLSRv2 routing protocol:

The original OLSRv2 does not provide security quantities in the protocol. OLSRv2 accepts that every node is supportive and kindly. This assumption is incorrect in a military environment. Malicious nodes can also attacks the good nodes. Based on trust values, a secure route can be established.

Change in OLSRv2 includes two important parts: route selection process based on link metrics and trust value calculation algorithms.

The proposed method use the **Dijkstra's algorithm** to calculate the best routing path. Since the minimization is used in the Dijkstra's algorithm, it is essential to convert the trust value to untrustworthy value. Then, minimize the untrustworthy value of a path using the Dijkstra's algorithm. To this end, It describes the untrustworthy value between node *A* and node *B* as U_{AB} which can be calculated as $U_{AB}= 1 - T_{AB}$.

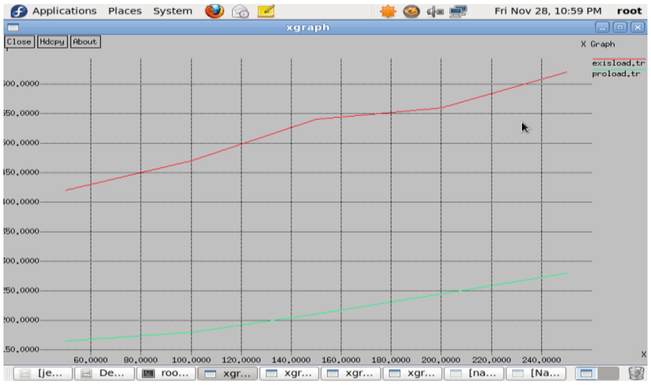
The sum of untrustworthy values of a path is,

$$U_{path} = \sum_{i=1}^{n-1} U_{k_i k_{i+1}} = \sum_{i=1}^{n-1} (1| - T_{k_i k_{i+1}}),$$

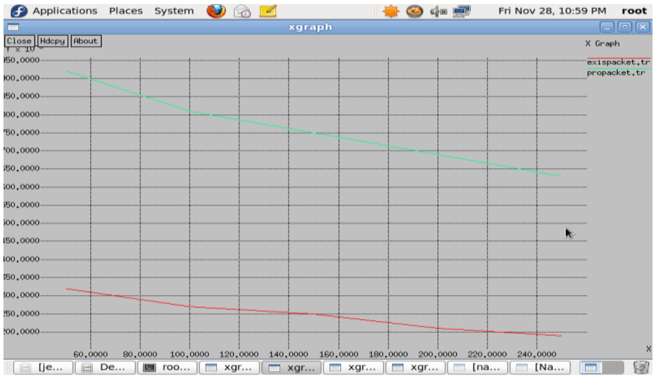
where $T_{k_i k_i+1}$ is the trust value between node k_i and its one-hop neighbor, node k_{i+1}. Nodes k_1,k_2,…….., k_n belong the path satisfies the minimum of U_{path}.
The trust values and routing table of each node can be maintained in the trust platform module (TPM), which provides additional security protection in open environments.

III. EXPERIMENTAL RESULTS

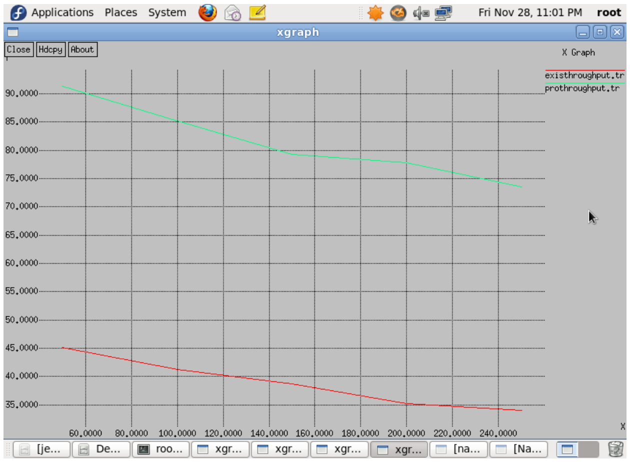
The implementation of trust management scheme that enhances the security in MANETs. The following scenarios are comparision results between existing and proposed scheme.



This graph explains that the existing routing load with proposed load. There is a routing load will decreases gradually when the number of nodes grows. The results shows that the proposed scheme has a lower routing load because of the higher number of packets are received correctly by destination node.



This graph explains that the existing packet delivery ratio(PDR) with proposed PDR. Here a packet delivery ratio can be decreases gradually when the number of nodes grows. The proposed scheme has much higher PDR than the existing scheme because best route has been determined by trust.



This graph explains that the existing throughput with proposed throughput. Here a throughput will be decreases gradually when the number of nodes decreases. The proposed scheme has much higher throughput than the existing scheme because of trust based routing algorithm. That improves the performance and throughput of OLSRv2.

IV CONCLUSION AND FUTURE WORK

The unified trust management scheme was implemented using recent progresses in uncertain reasoning. Bayesian inference and Dempster-Shafer theory are the methods of uncertain reasoning which estimate the trust values of observed nodes in MANETs. Misbehaviors such as dropping and modifying packets can be identified through the trust values by direct and indirect observation. Trust based routing algorithm will eliminate the nodes with low trust values. Therefore, secure routing path can be recognized in malicious environments. Based on the proposed system, more accurate trust can be found by considering different kinds of packets, indirect observation from neighboring nodes and other important issues such as queue length and states of wireless connections, which may root dropping packets in kindly nodes. The effects of MANET routing based on trust management surely support the effectiveness and performance of this scheme, which improves throughput and packet delivery ratio substantially.

Extend the proposed scheme with cognitive radios in MANETs. This includes additional security to MANET based on trust evaluation.

REFERENCES

[1]. Zhexiong Wei, Helen Tang, F. Richard Yu, Maoyu Wang, and Peter Mason "Security Enhancements for Mobile Ad Hoc Networks with Trust Management using Uncertain Reasoning" IEEE Transaction Vehicular technology, VOL. 13, NO. 3, 2014.

[2]. Bhavyesh Divecha, Ajith Abraham, Crina Grosanand Sugata Sanyal "Impact of Node Mobility on MANET Routing Protocols Models", Vol.3, No.1, july 2014.

[3]. Boun padith Kann havong, Hideshisa Nakayama, Yoshiaki Nemoto, Nei Kato – Tohoku university, Abbas Jamalipour – university of Sydney "A Survey Of Routing Attacks In Mobile Adhoc Networks", Vol.2, No.2, august 2001.

[4]. C´edricAdjih, Daniele Raffo, Paul M¨uhlethaler INRIA, Domaine de Voluceau, France1 "Attacks Against OLSR: Distributed Key Management for Security", Vol.2, No.2, july 2000.

[5]. Cedric Adjih, Thomas Clausen, Philippe Jacquet, Anis Laouiti, Paul M¨uhlethaler, Daniele Raffo "Securing the OLSR protocol", Vol.2, No.2, july 2000.

[6]. Huanyu Zhao, Xin Yang, and Xiaolin Li, Member, IEEE " cTrust: Trust Management in Cyclic Mobile Ad Hoc Networks" IEEE Transaction on Vehicular Technology, VOL. 62, NO. 6, July 2013

[7]. Philip England, Dr Qi Shi, Dr Bob Askwith, Dr.Faycal Bouhafs "A Survey of Trust Management in Mobile Ad-Hoc Networks", Vol.1, No.2, January 2013

[8]. 7.Quansheng Guan, Member, IEEE, F. Richard Yu, Senior Member, IEEE, Shengming Jiang, Senior Member, IEEE, and Victor C. M. Leung, Fellow, IEEE "Joint Topology Control and Authentication Design in Mobile Ad Hoc Networks With Cooperative Communications" *IEEE Transaction on Vehicular Technology*, VOL. 61, NO. 6, July 2012.

[9]. F.Richard Yu, Helen Tang, Peter C. Mason, and Fei Wang "A Hierarchical Identity Based Key Management Scheme in Tactical Mobile Ad Hoc Networks" IEEE Transaction on Network and service management, VOL. 7, NO. 4, December 2010.

[10]. Rui Zhang • Yanchao Zhang • Yuguang Fang "AOS: an anonymous overlay system for mobile ad hoc networks", Vol.3, No.1, july 2005.

[11]. Shengrong Bu, Student Member, IEEE, F. Richard Yu, Senior Member, IEEE, Xiaoping P. Liu, Senior Member, IEEE, Peter Mason, and Helen Tang, Member, IEEE "Distributed Combined Authentication and Intrusion Detection With Data Fusion in High-Security Mobile Ad Hoc Networks" IEEE Transaction on Vehicular Technology, VOL. 60, NO. 3, March 2011.

[12]. Shengrong Bu, Student Member, IEEE, F. Richard Yu, Senior Member, IEEE, Xiaoping P. Liu, Senior Member, IEEE, Helen Tang, *Member, IEEE* "Structural Results for Combined Continuous User Authentication and Intrusion Detection in High Security Mobile Ad-Hoc Network" IEEE Transaction on Wireless Communications, VOL. 10, NO. 9, September 2011.

[13]. Shohreh Honarbakhsh, Liza Binti Abdul Latif, Azizahbt Abdul Manaf, and BabakEmami "Enhancing Security for Mobile Ad hoc Networks by Using Identity Based Cryptography" International Journal of Computer and Communication Engineering, Vol. 3, No. 1, January 2014.

[14]. Thomas M. Chen and Varadharajan Venkataramanan, Southern Methodist University "Dempster-Shafer Theory for Intrusion Detection in Ad Hoc Networks",Vol.1, No.3, september 2000.

[15]. Thomas Clausen, Ulrich Herberg "Vulnerability Analysis of the Optimized Link State Routing Protocol version 2 (OLSRv2)" ,Vol.3, No.1, march 2005.

[16]. Yanwei Wang, F. Richard Yu, Senior Member, IEEE, Helen Tang, Senior Member, IEEE, Minyi Huang, Member, IEEE "A Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad hoc Networks" IEEE Transaction on Wireless Communications, VOL. 13, NO. 3, March 2014.