ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

An Advanced Security Enhancements for Cognitive Radio Networks with Trust Management

C.Kalaiselvan[1], Kavitha K[2]

Assistant Professor, Dept. of ECE, Pavendar Bharathidasan College of Engineering & Technology, Trichy, Tamilnadu, India[1]

PG Student [Communication Systems], Dept. of ECE, Pavendar Bharathidasan College of Engineering & Technology, Tamilnadu, India[2]

ABSTRACT: The distinctive features of Cognitive radios (CR) , including dynamic topology and open wireless medium, may lead CR suffering from many security vulnerabilities. In the proposed trust management 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. With indirect observation, also called second hand information that is obtained from neighbour 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. Combining these two components in the trust model, we can obtain more accurate trust values of the observed nodes in Cognitive radios. Simulation results show the effectiveness of the proposed scheme such as throughput and packet delivery ratio can be improved significantly with slightly increased average end-to- end delay and overhead of messages.

KEYWORDS: cognitive radio, security, trust management, uncertain reasoning

I.INTRODUCTION

With recent advances in wireless technologies and mobile devices, cognitive radios 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 centres. There are many risks in military environments needed to be considered seriously due to the distinctive features of CR ,including open wireless transmission medium, nomadic and distributed nature, lack of centralized infrastructure of security protection
In this paper we also recognize uncertainty in trust evaluation. Based on this interpretation, we propose a trust management scheme to enhance the security of CR. 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 exhaustibility of uncertain reasoning make it successful in many fields, such as expert systems, multi-agent systems, and data fusion

II.SYSTEM MODEL

Trust Model In CR

In this section, we describe the definition and properties of trust in CRs . Based on the definition, we depict the trust model that is used to formulate the trust between two nodes in CRs, and present a framework of the proposed scheme

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

Definition and Properties of Trust

Trust has different meanings in different disciplines from psychology to economy. The definition of trust in CRs is similar to the explanation in sociology, where trust is interpreted as degrees of the belief that a node in a network (or an agent in a distributed system) will carry out tasks that it should. Due to the specific characteristics of CRs, trust in CRs has five basic properties: subjectivity, dynamicity, non-transitivity, asymmetry, and context-dependency. Subjectivity means that an observer node has a right to determine the trust of an observed node. Different observer 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 behaviours. 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. Context-dependency means that trust assessment commonly bases on the behaviours 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 neighbours. 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.

Trust Model

Based on the de nition and properties of trust in CRs, 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 trustor needs to consider risk, 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. In direction observation trust, an observer estimates the trust of his one-hop neighbour based on its own opinion. Therefore, the trust value is the expectation of a subjective probability that a trustor uses to decide whether or not a trustee is reliable.

III. FRAMEWORK

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.

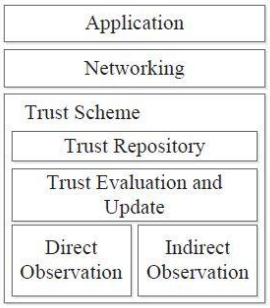

Fig 1: framework of the proposed scheme

i.Trust evaluation with direct observation

Based on the model presented in the last section, we evaluate trust values with direct observation on two malicious behaviours: dropping packets and modifying packets .In the direct observation, we assume that each observer can overhear packets forwarded by an observed node and compare them with original packets so that the observer can identify the malicious behaviours of the observed node. Therefore, the observer node can calculate trust values of its neighbours by using Bayesian inference, which is a general framework to deduce the estimation of the unknown

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

probability by using observation. As mentioned in the last section of trust model, the degree of belief is a random variable, denoted by T and 0<1. From Bayes' theorem, we can derive the following formulation

$$f(\theta, y|x) = \frac{p(x|\theta, y)f(\theta, y)}{\int_0^1 p(x|\theta, y)f(\theta, y)\,\mathrm{d}\theta},$$

where
x is the number of packets forwarded correctly;
y is the number of packets is received by node

ii. Trust Evaluation With Indirect Observation

In this section, indirect observation from neighbour nodes used to evaluate the trust value of the observed node will be discussed. Although direct observation from an observer is important in assessing the trust value of the observed node, the testimonies from neighbour nodes are also helpful to judge the trustworthiness of the observed node. Collection of neighbours' opinions can help in justifying whether or not a node is hostile. This mechanism may reduce the bias from an observer. A situation in which a node is benign to one node but malicious to others may be mitigated. In order to implement this method, the Dempster-Shafer theory, which is a mathematical theory of evidence, is used as it is well developed for coping with uncertainty or ignorance, and it provides a numerical measurement of degrees of belief about a proposition from multiple sources.

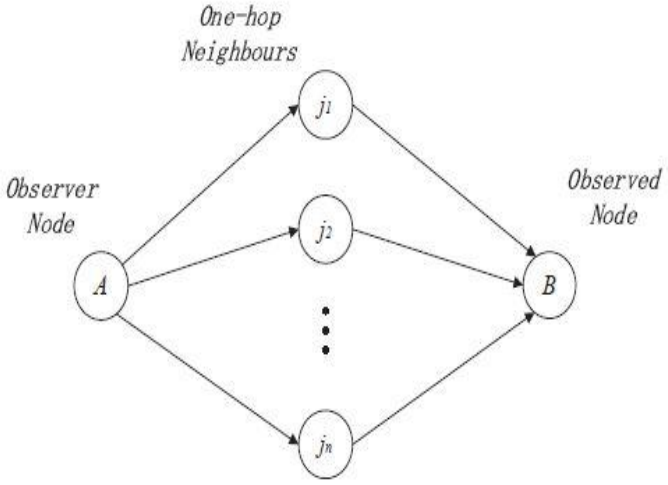

Fig 2: A scenario for indirect observation

iii. Secure routing based on trust

The original OLSRv2 does not provide security measurements in the protocol. OLSRv2 assumes that every node is cooperative and benevolent. However, this assumption inappropriate in a military environment. Malicious nodes can attack nodes that are not protected. Based on trust values, a secure route can be established.

Modifications of OLSRV2 include two important parts: route selection process based on link metrics and trust value calculation algorithms. Although OLSRv2 provides new features such as link metrics and extensible message formats, which may be used to improve security of the protocol, OLSRv2 implementation still attempts to use hop count when the shortest routing path is calculated. In order to implement route selection process based on link metrics, there are three components that need to be changed, HELLO and TC messages, protocol information bases, and the shortest path algorithm. Message format is extensible and flexible in OLSRv2. Thus link metrics information can be

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

added to messages as Type Length Value (TLV) blocks. Modification of protocol information bases, including local information base, neighbour information base and topology information base, is used to record link metrics in each node. Based on these information bases, route processing set can update the shortest routing path with link metrics.

Algorithm 1 Trust Calculation with Direct Observation

```
1: if node A, which is an observer, finds that its one-hop
   neighbor, Node B that is a trustee, receives a packet then
2:   the number of packets received increases one
3:   if node A finds that node B forwards the packet suc-
     cessfully then
4:     the number of packets forwarded increases one
5:   else
6:     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
7:       the number of packets received decreases one
8:     end if
9:   end if
10: end if
11: calculate the trust value, T^S, from (8) and update the old
    one.
```

Algorithm 2 Trust Calculation with Indirect Observation

```
   if node A, which is an observer, has more than one one-
   hop neighbors between it and the trustee, node B then
2:   calculates the trust value, T^N, from (18)
   else
4:   set T^N to 0
     set λ to 1
6: end if
```

IV. RESULTS AND DISCUSSION

i.Environment Settings

We randomly place nodes in the noted area. Each scenario has a pair of nodes as the source and destination with Constant Bit Rate (CBR) traffic. 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. In this adversary mode, the proposed scheme is evaluated and compared with the original OLSRv2 protocol. We have simulated networks with different numbers of nodes. Fig. 3 is an example of the network setup where node 1 is the source node that generates the CBR traffic

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

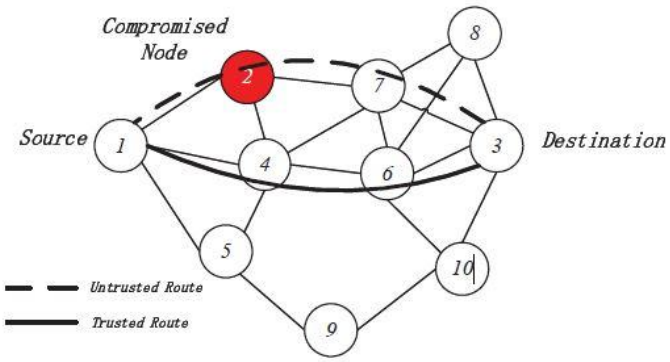

Fig 3: an example of the network setup

There are four 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) Average end-to-end delay is the mean of end-to-end delay between a source node and a destination node with CBR traffic; 4) Message Overhead is the size of Type Length Value (TLV) blocks in total messages, which are used to carry trust values; 5) Routing load is the ratio of the number of control packets transmitted by nodes to the number of data packets received successfully

ii. Performance Improvement

The original OLSRv2 and our scheme are evaluated in the simulations, where some nodes misbehave through dropping or modifying packets. we compare our scheme with and without indirect observation and original OLSRv2 in scenarios that a source node sends data packets to a destination node in the network, which includes nodes from 5 to 30

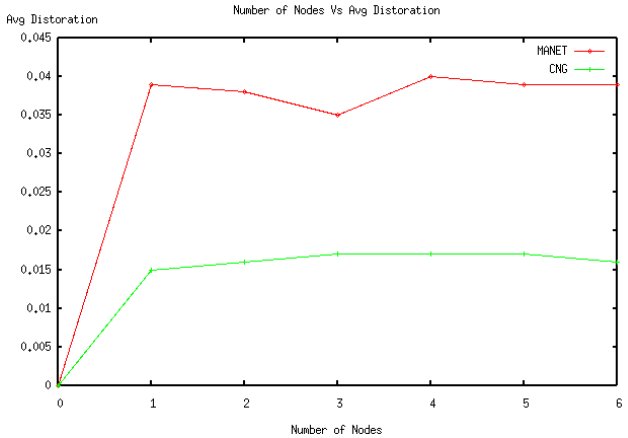

Fig 4: No.of nodes vs average distortion

Fig 4 shows the no.of nodes vs average distortion. The average distortion occurred within the network with respect to the total number of nodes and it shows less distortion than in MANET

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

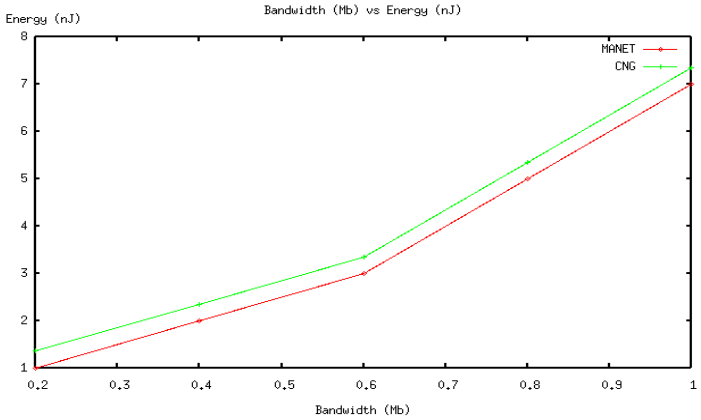

Fig 5: bandwidth vs energy

Fig 5 shows the bandwidth vs energy. The difference between CNG and MANET network is only slightly varied in the bandwidth and energy allocation

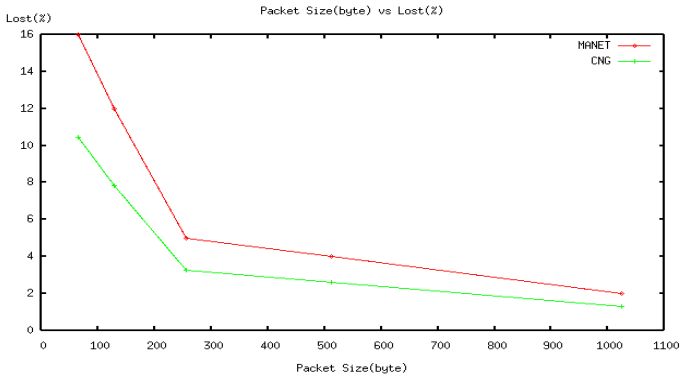

Fig 6:packet size vs lost

Fig 6 shows the packet size vs lost. Packet lost is the one in which the packet is lost due to traffic or other reasons. It is also low when compared with MANET

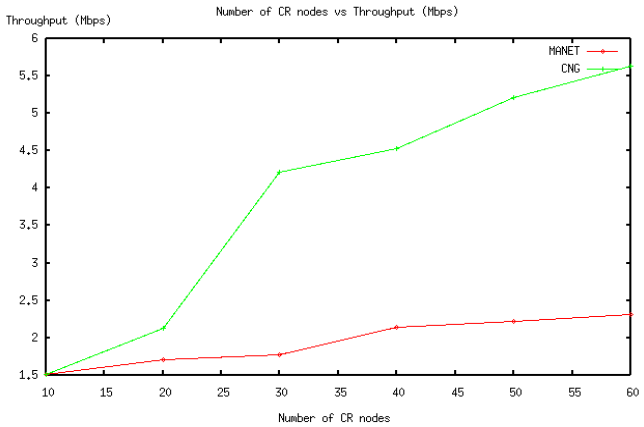

Fig 7: no.of nodes vs throughput

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

Fig 7 shows the no of nodes vs throughput. Throughput is the average rate of successful message delivery over a communication channel.

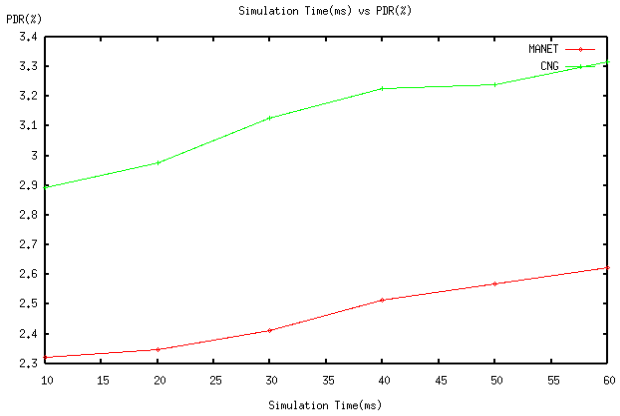

Fig 8:simulation time vs PDR

Fig 8 shows the simulation time vs PDR. PDR is the Packet Delivery Ratio defines the ratio of sending and receiving packet within the channel

V.CONCLUSION

The proposed system uses the recent advances in uncertain reasoning, Bayesian inference and Dempster-Shafer theory, we evaluate the trust values of observed nodes in Cognitive radios. Misbehaviours 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 neighbours 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 Cognitive radios 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

REFERENCES

[1] J.H.Cho, A.Swami and I.R.Chen, "A Survey on trust management for mobile ad hoc networks", IEEE communications surveys and tutorials,vol.13,no.4,pp.562-583,2011
[2] Y.Zhang, W.Liu, W.Lou, Y.Fang, "Security mobile ad hoc networks with certificateless public keys", IEEE Trans.Dependable and secure computing, vol.3, pp.386-399,oct 2006
[3] Kwang-chengchen, Peng-yu-chen, Neeli Prasad and Sumei sun, "Trusted Cognitive radio networking" IEEE Wireless Comm.Mob.Comp,2009
[4] A.Sumathi and R.Vidhyapriya, "Security in cognitive radio networks-a survey", Intelligent Systems Design and Applications (ISDA), 12th international conference, pp.114-118, Nov 2012
[5] R.Chen, J.M.Park, J.Reed, "Towards secure distributed spectrum sensing in cognitive radio networks", Communications Magazine, IEEE vol.46,no.4,pp 50-55,april 2008
[6] F.Adelantado and C.Verikoukis, "A non-parametric statistical approach for malicious users detection in cognitive wireless ad hoc networks",IEEE International conference (ICC), pp.1-5,june 2011
[7] J.Burbank , "Security in cognitive radio networks: The required evolution in approaches to wireless network security", CrownCom, 3rd international conference, pp 1-7, may 2008
[8] N.Prasad, "Secure cognitive networks in wireless technology" , EuWiT, European conference, pp.107-110, oct 2008