ISSN No. 0976-5697

Volume 2, No. 3, May-June 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Enhancing Malfunction Resilience in Cognitive Radio Networks

Vibhakar Pathak*
Dept. of Information Technology
Suresh Gyan Vihar University
Jaipur,India
vibhakarp@rediffmail.com

Dr. K C Roy
Dept. of ECE
Pacific University
Udaipur,India
roy.krishna@rediffmail.com

Santosh Kumar Singh
Dept. of Information Technology
Suresh Gyan Vihar University
Jaipur,India
sksmtech@yahoo.com

Abstract:- This paper proposes a malfunction resilient protocol for routing based on COGNET and Cross Layer Aware(CLA) architectures . Different from existing solutions Cog-CLAR(Cognitive- Cross layer Aware Routing) , does not focus on a particular attack or malfunction but instead takes generalized approach. Cog-CLAR achieves resilience against a range of routing disruption by treating them as "dysfunctional " networks ,denote link and routing failures caused by link contention or node mobility. Cog-CLAR is a cross layer scheme that detects attacks or malfunction at the transport layer but responds to them at the network layer or MAC layer . Because dysfunctional network events and disruption attacks have pronounced effect on the size of transport layer congestion window and flow monitoring of G C P(Global Control Pane of COGNET architecture) monitoring such is an effective method of detecting such event using this method Cog-CLAR is able to detect attacks or malfunction . Once attack is detected Cog-CLAR initiate cognitive radio function or re-routing that circumvents and bootstrap the nodes that are likely to be misbehaving. Analysis and simulation results show that Cog-CLAR is effective in the monitoring a number of malfunction or insider as well as jelly fish (JF) attack our results indicate that Cog-CLAR is also effective in improving network throughout because its proactive cognitive radio function aids in maintaining a reasonable level of throughout when dysfunctional network events occurs.

Keywords: Cognet, DoS, cross-layer, jelly-fish ,DSR ,OMNET++

I. INTRODUCTION

In a Cognitive Network, wireless devices communicate by sensing physical parameters, changing radio and forwarding packets on behalf of other devices-there is no central base station or fixed infrastructure to handle data routing. Cognitive Networks are particularly useful when a fixed infrastructure (e.g, a base station or access point),radio is impractical due to space , time or spectrum constraints or when an existing infrastructure is not suitable for the required task. For mission –critical and other information – sensitive applications, the dependability and security aspects of the Cognitive Network .including reliability and availability, are of great importance. Denial of service (DoS) attacks and PU (Primary User) demand is a major threat to security and quite a few of them have been discovered and discussed in the literature. Among them, routing disruption attacks are particularly menacing since they attempt to cause legitimate data packets to be routed in a dysfunctional way. Routing disruption and DoS attacks can be divided into three categories based on their different levels of sophistication: outsider attacks, insider attacks, and protocol-compliant attacks. In an outsider attack, the attackers are assumed to have no knowledge of the keys that are used to encrypt and authenticate the data and routing control packets. Preventing outside attackers from tampering with the data is accomplished by simply employing encryption and authentication schemes. In an insider attack, an attacker has compromised or captured a node, thus gaining access to encryption and authentication keys. The primary method of detecting and mitigating insider attacks is to monitor the packet forwarding behavior among the nodes [2],[3],[10],[12]. Also, there are approaches that focus on thwarting specific forms of insider attacks [6],[7]

Protocol-compliant attacks are the most difficult to defend against. In [1], Aad et al. refer to such attacks as "JellyFish" (JF) attacks. While the two types of attacks discussed above disobey protocol rules, JF attacks conform to all routing and forwarding rules. They are also passive, and therefore difficult to detect. A typical target of JF attacks is closed-loop flows that respond to packet delay and loss, such as TCP. Protecting Network against JF attacks is a formidable task that has yet to be addressed.

We propose a routing architecture for CRN, called Cognitive-Cross layer Aware Routing(Cog-CLAR), which is resilient against a wide range of attacks, including protocol-compliant attacks. Cog-CLAR a cross-layer approach that monitors the variations in the size of the TCP congestion window , Flow monitor of GCP of COGNET system to detect abnormalities and reacts to those abnormalities at the network layer by initiating a re-routing process. The Cog-CLAR architecture is compatible with on-demand source routing protocols such as Dynamic Source Routing (DSR) [8]. Cog-CLAR is composed of three modules: the *congestion window monitoring (CWM)* module, GCP *flow monitor* (FM) module and the *Bio inspirsed re-routing (BRR)* module. CWM is responsible for detecting any abnormalities that might occur on a route and FM for abrupt radio change. If any abnormalities are detected, CWM or FM invokes BRR to build a new route. Our simulation results show that Cog -CLAR can effectively mitigate protocol-compliant attacks. Moreover, results indicate that Cog-CLAR is capable of circumventing a variety of insider attacks.

The remainder of this paper is organized as follows. Section II provides the technical background of Cog-CLAR. Section III introduces Cog-CLAR and its modules. The simulation results are shown in Section IV. Finally, we conclude the paper in Section V .

II. TECHNICAL BACKGROUND

A. Related Work

Spoofing and replay are typical outsider attacks. They can be countered with encryption and packet authentication. Schemes that employ encryption or authentication include the secure Routing Protocol (SRP) [11] and Ariadn [5] . The SRP attaches a security extension header to each control packet. SRP can be used for the DSR using a variant of the TESLA source authentication technique. Various insider attacks have been discussed in the literature, including blackhole, grayhole [5] rushing [7] wormbole [6] blackmail, and selfish attacks,. The research community has made a great effort to combat insider attacks [2],[3],[6] [7] ,[10],[12]. Awerbuch et al. [2] introduced a technique for detecting faulty links on a path from the source to the destination using a binary search. Hu et al. Proposed the Rushing Attack Prevention (RAP) scheme (7) as a generic defense against the rushing attack for protecting non –demand routing protocols. The same authors proposed “packet leashes”[6] to thwart wormhole attacks during a route search process. A reputation based system is another approach that thwarts attacks by monitoring the network traffic [3] ,[10] ,[12] . For example, Martie et al. .[10] proposed two modules “watchdog” and “pathrater” for this purpose. Watchdog is a module that detects neighbor nodes’ misbehavior in the promiscuous mode; and pathrater is a route selection module that define a route’s quality as the average reputation of the nodes on the route and chooses the route with the best quality. Protocol compliant DoS attacks, a.k.a JF attacks [1] is by far the most difficult to defend against. In a JF attack, the malicious node can reorder packets, periodically drop packets, or increase packet jitter. Although such behavior can be considered a network layer attack, it affects the transport-layer good put by exploiting the vulnerabilities of the congestion control mechanism. It was shown in that the JF attack can result in near zero good put in the transport layer while keeping network-layer throughput fairly stable. Currently there is no known counter measure for the JF attack. As primary user emulation or demand . In this situation Cognitive Radio Network has to change parameter at PHY,MAC level resulting in data loss or denial of some quality parameter due to adjustment of frame size. The attack of PU emulation can be detected at PHY by using HPB (hyperbolic Position Bounding),Time arrival and other various location and orientation detection methods. Apart from Denial of Services(DoS) attack Coginitive radion network also has protocol compliance

a) Overview of the Dynamic source routing protocol

Cog-CLAR is an architecture for secure routing in Cognitive Network that can be most readily integrated into on demand source routing protocols. To describe Cog-CLAR functionalities in a concrete way, we will discuss it in the context. Of an actual on –demand source routing protocol, namely DSR [8] uses the source routing option in data packets to carry the routing information. Each node, using a route cache, stores one or more complete lists of node addresses that form a path toward a destination. DSR is composed of two phases: route discovery and route maintenance.

Route discovery: When a node has packets to send, it first checks its route cache. If a route entry corresponding to the destination is not present in its rout cache, a ROUTE REQUEST packet is broadcast over the network. The ROUTE request packet is uniquely identified by the source address, the destination address, and a sequence number that is incremented by the source node for each route discovery request. An intermediate node appends its own address to the node list in the Route Request packet and forwards it. When the Route Request packet reaches the destination node, it has accumulated the path form the source to the destination. Assume that the underlying MAC layer supports bidirectional links, the destination node can get a valid route back to source node simply by reversing the source route recorded in the Route Request packet. Then the destination node send s back to the source node Route Reply packet along the same route in the opposite direction. The Route Reply packet contains the information needed fro the source node to route its packets to the destination node. It is possible for a node to receive the same Route Request packet multiple times because it is broadcast over the network. DSR requires an intermediate node to respond only to the first Route Request packet received and ignore the other duplicates, which is known as “duplicate suppression” Note that duplicate suppression makes DSR vulnerable to rushing and wormhole attacks-if a malicious node manages to disseminate Route Request packets quickly so that they reach the other nodes before the legitimate packets, then the malicious node on a route with the least delay will always be included in the selected route.

Route maintenance: Every node along a route is responsible for the validity of the downstream link connecting itself and its next hop node. If link breakage is found, the source node will be notified with a Route Error packet. The source node then initiates another route discovery procedure. Note that this procedure has a vulnerability: since sending a Route Error packet is voluntary, malicious nodes can break links without being detected by the source node.

b) Overview of the Cognitive Cross layer Routing

This is a cross layer aware routing protocol develop by authors [7] . In this information about channel state , observed link state and hop by hop reasoned and observed information are utilized by network layer protocol in general and routing algorithm in specific .Exactly Signal to interference and noise ratio(SINR) , received power(RP) , delay observed by reactive ant, pheromone value, knowledge based interpolation are passed on to routing algorithm for decisions for source routing between source and destination . The protocol improves over another cross layer protocol by employing ANT colonization approach for optimization and knowledge based reasoning for decision support .Apart from decision in proactive routing it can also adapt as per reconfigurability of PHY or flexibility provided by agile radio.

The protocol is based on source routing with additional information and decision parameters from PHY and MAC

Layer. The protocol has very simple two fold approach. First fold use to discover the route ,which is as.

1. A small packet known as ANT is sent to discover new route.
2. ANT places small amount of data containing PHY and MAC observed information on to every node it traverse. It is just like ANT leaving pheromone in the route.
3. If ANT found destination route without broadcast. It can be thought as optimal route.
4. If ANT stuck at any node it broadcast with threshold 2 which guarantee non flooding of network and producing sub optimal alternate route.

In second fold the pheromone placed at each node is used by reasoning engine for short term prediction on link state and route condition in hop by hop basis . which is use to adapt optimize various communication parameter based on AgileMAC protocol develop by authors [4] .

III. THE COGNITIVE CROSS LAYER AWARE REROUTING

The basic protocol develop for re-routing is based on BioCLAN developed by the author[9]with additional service of Flow Monitor(FM). The flow monitor is use to track change in flow rate and report various physical parameter change to the routing system in case of abrupt eviction status following attack condition of protocol complaint attack at agile radio level. We assume all links in the network to be bidirectional. We only consider network-layer route disruption attacks and disregard attacks to the physical or link layer of a wireless network. In a communication session, we assume that both the source node and the destination node are trustworthy but intermediate nodes are not. It is assumed that all control packets used in Cog-CLAR are authenticated via certain security mechanism (e.g., [5], [11]). Under this assumption, Cog-CLAR is inherently resistant to outsider attacks. We focus our discussions on insider attacks and protocol-compliant attacks. A route with one or more malicious nodes is considered an “infected” route. In this paper, we focus on TCP as it is the most widely-used transport-layer protocol and it is the attack point of JF attacks. Cog-CLAR uses a CWM module to observe the variations in the size of the TCP congestion window. If the variation indicates an abnormality, an alarm is raised to activate the BRR module. The BRR module in turn finds a new route. Cog-CLAR strengthens the two vulnerabilities of DSR. First, Cog-CLAR fortifies the “passive” re-routing approach of DSR by supporting both passive re-routing and a form of “active” re-routing. In DSR, the source node passively waits for a ROUTE ERROR packet to trigger a re-routing process. Cog-CLAR enables the CWM module or FM to actively initiate a re-routing process when network abnormalities are detected. Therefore, even if a malicious node on an infected route drops ROUTE ERROR packets, the source node is able to initiate re-routing. Second, Cog-CLAR facilitates the process of identifying a valid route when a new route has to be found.

BRR enhances the re-routing functions in three aspects. First, when CWM detects any abnormalities in a route, BRR tags the current route as an infected route. If there is no non-tagged route available in the source node’s cache, BRR initiates an active re-routing process based on BCLAN [9] rather than just responding passively to Route Error packets. Second, during the active re-routing process, the source node collects more routing information by disabling duplicate suppression Third, with the route information in its cache, the source node selects a new route using the following BRR algorithm. Apart from above BRR also monitor flow or sliding windows size ,to get idea of PU’S demand or PU emulation attack

Assume that the source node’s set of cached uninfected routes are represented by SN = , where U= denotes the number of elements in set X) , and the routes that are tagged as infected are represented by Sr= where M= Here, Nj or Ri denotes a set of nodes contained in a given route. Let us define the “alikeness degree” of Nj with respect to Sr to be E(j)=max then, BRR algorithms can be expressed as follows: the sender selects a new route by selecting a route in the cache with the smallest alikeness degree. That is it selects a new route Nj such that j = argmin (E(j) if there are multiple routes that satisfy the aforementioned condition, then the one with the least number of nodes is selected among them. If there are still more than one routes to choose from, then the one with the smallest index is chosen.

BRR also checks flow or sliding window size on GCP to check abrupt eviction of nodes in following manner.

(i) If flow window or sliding window of GCP has slow response then a condition of abrupt eviction can be thought

(ii) If sender sliding window has higher window size from operative states with smaller value of receiver or piggybacking window then a condition of eviction by PU ‘s demand or PU emulation attack is there

For condition (i) a Bootstrapping of node with new physical parameter suffice the case of re-routing.

For condition (ii) a bootstrapping followed by Go Back N protocol for re-routing.

IV. SIMULATION STUDY

After *A. Simulation Environments*

The simulation results shown in this section were obtained via omnetpp . We consider a network of 125 nodes in a 1500m x 1500m square area. Nodes use the 802.11 MAC with a 250m communication range. Each node moves according to the random waypoint model, which repeats the following four steps:

1) It randomly chooses a destination in the area with a uniform distribution;

2) It chooses a velocity *v* that is uniformly distributed over [*vmin, vmax*];

3) It moves along the straight line from its current position to the destination with the velocity *v* until it arrives; and

4) It pauses in the destination for a random period that is uniformly distributed over [0*, tmax*].

We adopted the values *vmin* = 15*m/s*, *vmax* = 30*m/s*, and the *tmax* = 10*s*. With this model, ten different random movement patterns were generated. All of the results to be presented are averaged over five independent simulations on each of the ten movement patterns. We simulated 5-flow networks with 0, 16, 25, and 49 malicious nodes. The flows use TCP senders with standard TCP receivers. Each flow sends packets at a rate of 3000 bytes per second. Malicious nodes launch a *Periodic Drop JF attack* in which JF nodes forward all control packets and drop data packets for 300ms in every one second interval. We chose the period of one second because the Periodic Drop JF attack with this period length was shown to have the most detrimental effect on TCP goodput according to the results published in [1]. The values used for the number of nodes, flows and malicious nodes are the same as those used in the simulation experiments of [1]. Each simulation run lasts 500 seconds.

B. Simulation Results

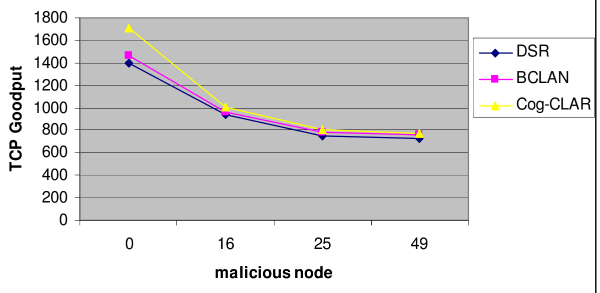

Fig 1 TCP Goodput

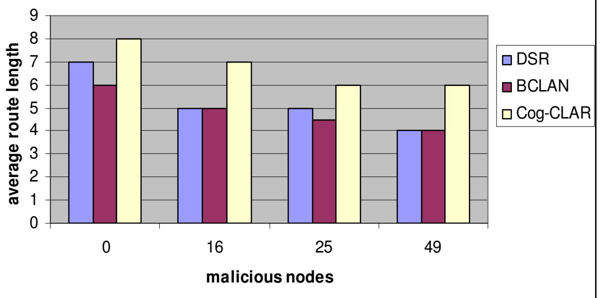

Fig. 2 Average route length

1) Data Throughput Figs. 1 DSR,BCLAN and COG-CLAR in terms of data throughput (i.e., goodput) and control overhead, respectively. Fig 1 shows that COG-CLAR achieves an increase in TCP goodput compared to DSR.and BCLAN Note that even when there is no malicious node, COG-CLAR increases the TCP goodput by 12%. This observation can be attributed to the fact that COG-CLAR actively conducts rerouting when node mobility causes link breakage, while DSR passively waits for ROUTE ERROR messages before initiating

Fig. 1. TCP goodput. re-routing. The goodput gain achieved by COG-CLAR decreases as the number of malicious nodes increases because the increase in the number of malicious nodes rapidly decreases available network resources.

2) Average Successful Route Length: The route length averaged over all successfully transmitted packets is an indicator of a protocol's ability to maintain multi-hop routes. Note that longer multi-hop routes are more vulnerable against routing disruption attacks. Fig. 2 shows that the average route length, measured in number of hops, is longer using COG-CLAR than using DSR under all scenarios, indicating that COG-CLAR is more resilient against attacks

V. CONCLUSIONS

This paper presented a novel routing architecture for CRNs called COG-CLAR that is attack resilient. COG-CLAR employs a cross-layer approach in that it uses the CWM module to detect network abnormalities (either attack or dysfunctional events) at the transport layer and responds to them by using the LAR module to execute re-routing at the network layer. Our analysis shows that COG-CLAR is resilient against a variety of insider attacks as well as protocol-compliant attacks. Simulation results show that COG-CLAR is effective in mitigating JF attacks in certain network environments. As part of our future work, we will explore the possibility of adapting the principles of COG-CLAR to routing protocols other than DSR and BCLAN.

VI. REFERENCES

[1] I. Aad, J. Hubaux, and E. W. Knightly, "Denial of service resilience in ad hoc networks," *Proc. MobiCom*, Sep. 2004, pp. 202-215.

[2] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An on demand secure routing protocol resilient to Byzantine failures," *Proc.WiSe*, Sep. 2002, pp. 21-30.

[3] S. Buchegger and J.-Y. Le Boudec, "Nodes bearing grudges: towards routing security, fairness, and robustness in mobile ad hoc networks," *Proc. 10th Euromicro Workshop on Parallel, Distributed and Network based Processing*, Jan. 2002, pp. 403-410.

[4] Vibhakar Pathak, K C Roy , Santosh K Singh , "Cross layer aware adaptive MAC based on knowledge based reasoning for cognitive radio computer network " in International Journal of Next-Generation Networks Vol. 2,No.2,June2010 pp. 14-21

[5] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A Secure on-demand routing protocol for ad hoc networks", *Proc. MobiCom*, Sep. 2002, pp.12-23.

[6] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," *Proc. INFOCOM*, Mar. 2003, pp.1976-1986.

[7] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," *Proc. WiSe*, Sep. 2003,pp. 30-40.

[8] [D. B. Johnson, D. A. Maltz, and Y.-C. Hu, *The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR) (Internet-Draft)*, Mobile Ad-hoc Network (MANET) Working Group, IETF, July 2004.

[9] Vibhakar Pathak, K C Roy , Santosh K Singh ," Bio Inspired Cross Layer Aware Network protocol for Cognitive Radio Networks" in Global Journal of Computer Science and Technology Vol. 10 Issue 12 Oct 2010 pp. 92-95

[10] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," *Proc. MobiCom*, Aug. 2000, pp. 255-265.

[11] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," *Proc. CNDS*, Jan. 2002.

[12] W. Yu, Y. Sun, and K. J. R. Liu, "HADOF: Defense against routing disruptions in mobile ad hoc networks," *Proc. INFOCOM*, Mar. 2005, pp.1252-1261.