Security Attacks and Counter Measures on Network Layer in Cognitive Radio Network: A Review

Manoj R
Assistant Professor-Senior Scale,
Department of CSE
Manipal Institute of Technology,
Manipal University, Manipal, India,
manoj.r@manipal.edu

Dr. Harish S V
Professor,
Department of CSE
Manipal Institute of Technology,
Manipal University, Manipal, India,
harish.sv@manipal.edu

Shyam S Karanth
Assistant Professor Senior Scale,
Department of CSE
Manipal Institute of Technology,
Manipal University, Manipal, India,
shyam.karanth@manipal.edu

Abstract - Cognitive Radio (CR) is used to represent integration of substantial, computational intelligence particularly in machine learning, vision and natural language processing into software defined radio. Ideal Cognitive Radio is CR with autonomous machine learning, vision and spoken or written language perception [1].Spectrum shortage is a major problem in wireless communication. Our paper focuses on the existing attacks and security issues in CR Networks on network layer. The fundamentals of CRNs including the basic components, study on the various network layer attacks like Hello flood, Sink Hole, Ripple, Wormhole and their Defense are reviewed [2]. In CR we need to first identify the requirements of protocol for network layer of Cognitive Radio Network, propose a protocol for Defense of attacks, design, implement and evaluate the best effort Network protocols [3]. The scope of this survey is to present an overview of the security threats and challenges on Network Layer in Cognitive Radio. We also presented attack scenarios specific to Cognitive Radio Network architecture and capabilities. Following each attack scenario, we presented mitigation techniques particular to the attack.

Keywords—Cognitive Radio,Network Layer, Security,Attacks,Countermeasures.

I. Introduction

The increase in wireless devices such as smartphones, laptops, tablets has caused the frequency spectrum to become crowded. Currently, frequency spectrum has divided into 2 main categories: licensed and unlicensed. Licensed spectrum is reserved for specific users and is usually underutilized. Since unlicensed spectrum is available for public , the spectrum has become overcrowded. Spectrum Overcrowding is one of the major challenges in wireless industry .One such solution to solve the crisis of spectrum overloading and proper utilization of spectrum is the Cognitive Radio[CR]. This technology is based on IEEE standard 802.22. CR is vulnerable to several attacks because of its ability to sense the environment ,adjust spectrum according to different parameters. This Paper extends its approach to Network Layer in the study of Cognitive Radio Network and Security. Threats and strategies to detect and defend these threats are presented in this paper.

II. Cognitive Radio

Cognitive Radio is a software defined radio with adjustable parameters. Cognitive Radio is a wireless communication system that is aware of its surroundings and adapts its parameters accordingly. CR has the ability to detect the spectrum holes in licensed band and allow the secondary user to communicate through that band thus utilizing the spectrum effectively.

III. Cognitive Radio Networls Capabilities

A CR can sense and detect the holes present in the spectrum which are those frequency bands which are not being used by the primary or licensed user. It can share the spectrum under the terms and agreement with a license and third party. It also has a mechanism that allows CR to determine its location and location of other transmitters which can help in selecting different parameters. Its ability to discover and determine the available networks around it helps in best way of communication.

IV. Reconfigurable Capability

There are different parameters that a CR change to adjust according to the environment.CR has the ability to change the operating frequency dynamically to adjust according to the sensed information. Adaptive Modulation technique and Transmit Power control are other feauters that enables improved and effective usage of spectrum

V. Network Layer

Network Layer is responsible for packet forwarding and routing the packets through the best possible route available at that very instance. It provides facility to route the data from source in a network to destination in another network

VI. Attacks

.Because of different abilities of CR, it is more vulnerable to different attacks thus making more complication in providing security against these attacks. Table 1 provides a overview of different possible network layer attacks.

A. Sinkhole

It is easy to find loop holes in the network due to this routing which will affect the communication. The goal of adversary behind this attack is to attract all the nearby traffic by creating a trust base so as to pass all the traffic through the compromised node [9] thus allowing attacker to monitor or modify the packets. Attacker with a transmitter having enough power to reach the destined base station in a single hop can advertise itself as a high quality or best route (see Fig 1). Hence the neighboring nodes will forward their packets through the compromised node [5].Sinkhole attacks are

TABLE 1: NETWORK LAYER ATTACKS

Attack Name	Network Member	Description	Prevention	Advantage	Disadvantage
Sinkhole	Internal	Attacker proposes itself as best route and employs selective forwarding in which packets are either forwarded or discarded.	Authentication and encryption (for external attack). Trust based system (for internal attack).	(Empty)	(Empty)
Wormhole	Internal	Attacker forward messages or pieces of message to different part of network recursively.	Graphic routing protocols.	Easy Detection of damaged node	(Empty)
Hello Flood	Internal	Attacker has sufficient energy to broadcast Hello message to all nodes in network to convince them its their neighbor while it is very far away.	Maintaining session keys.	Limits the scope of attacker and is very effective in a given domain	Involves Trade-off between communication and security.
			Cryptographic methods.	Easy to implement.	Not a good preventive method can be by-passed easily (only cryptography is not enough for security).
			Probabilistic based approach.	Sensor node energy utilization is minimal.	Attacker might not be detected.
Sybil	Internal	Different identities are used by attacker.	Identity validation	(Empty)	(Empty)

characterized into two categories: Internal attacks and External attacks

Counter measures

Outside or external attack can be prevented by using authentication and encryption. Only authorized nodes will be able to join the network thus preventing an outside attacker to join it [5].

A(Empty)

D: (Empty)

Insider attack can be prevented by using a trust based system. CR monitor all the packets and passes the issues to Fusion center which analyses and flood the network with the issues recently experienced. Hence dropping the attacker out of the network based on results.

A: (Empty)

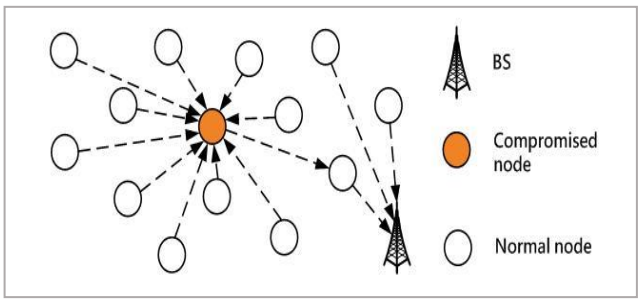

Fig. 1. Sinkhole Attack

D: (Empty)

B. Wormhole

In this attack, the compromised node tunnels a message in a part of network over a low latency link. Generally this attack consists of two or more nodes situated distantly in the network having a secret understanding about their distances by relaying packets along a channel which is only available to the attacker. Wormhole attack can also lead to sinkhole attack if one of the compromised node multiple hopes away from base station convinces neighboring nodes that it is single or two hopes away from a base station thus attracting more traffic. Wormhole can convince two distant nodes that to be each other's neighbors [5] (see Fig 2).

Countermeasures-

Geographic routing protocols can be used as a mitigation for wormhole attacks. Physical information of nodes can help in detecting the artificial link in the network thus preventing traffic to attract towards the wormhole or sinkhole

Advantage: Easy detection of compromised node

Disadvantage: (Empty)

Packet leashes method [5] can be used to detect and defend against wormhole attack.

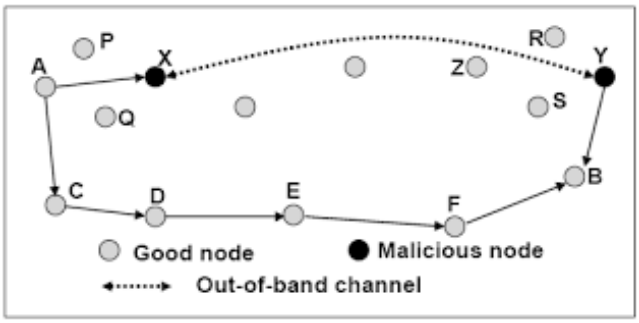

Fig. 2. Wormhole Attack

Leash is an information regarding the geographical location that is embedded in the packet. Sender includes transmission time and its location in the message. Receiver checks its clock and the distance travelled by the packet thus restricting the transmission distance [6].

A: (Empty)

D: (Empty)

C. Hello Flood

The attack is initiated by an attacker that broadcasts a message to all nodes in a network. This packet is used to direct the traffic to a specific destination claiming to be a high quality link. Sufficient energy is used to convince each node that the attacker is their neighbor. As a result the affected nodes receiving the packets assume that attacker is very close due to the strength of the received signal, when in fact the attacker is a great distance away. The attacker needs only to capture and rebroadcast overheard packets with enough power to reach every node in the network. Protocols which depend on localized information exchange between neighboring nodes for topology maintenance or flow control are mainly affected by this type of attack.

Countermeasure-

- Verification of bi-directionality can be established by maintaining session keys between two nodes or communicating parties in the network[3] .Keys allow to verify identities of the two nodes during communication and also provide an encrypted link between them. But these keys are limited which will in-turn prevent the attacker from establishing connection between every node. Alarm is signaled upon identification of an attacker. This method is very effective to identify the attacker in a particular region and it limits the scope of attacker in communication domain. The drawback of this approach is that there is a tradeoff between communication and security since the session keys are limited we are limiting the communication among the nodes, that is, one node can only communicate to limited number of resources also the establishment of encrypted link is expensive.
- In [7] hello flood attack is prevented with the help of cryptographic methods. In a network every two sensors will share the identical secret key. New encryption key is generated during the communication process. This phenomenon ensures that only reachable nodes can decrypt and verify the message and hence prevent the adversary from attacking the network. The method is easy to implement. Limitation of this approach is that it is a very simple method and can be manipulated easily for example any attacker can falsify its identity and can use it to generate attacks.
- Taking the scarcity of energy resources of sensor nodes into consideration, the authors have proposed in [8] a probabilistic based approach, in which few randomly selected nodes are forced to report to base station about requests made by the hello flood attacker. The base station then analyzes the request authenticity and detects for the presence of attacker. Utilization of energy resources of sensor nodes is minimal and method is easy to implement. The limitation of this approach is that probabilities computed are not absolute and also as we are forcing randomly selected nodes to report to base station it may happen that these are were not affected from hello requests but other nodes were in which the attack might go undetected.

D. Sybil

In a Sybil attack, the attacker affects the reputation system of network by creating a large number of anonymous . [9]In this attack a malicious user attains numerous sensor identities (see Fig 3). This can be done in two ways: Either other acquiring other sensors identities or creating new fake identities. It depends on following factors: Methods involved in creating identities, the degree to which the reputation system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, whether the reputation system treats all entities identically

A: (Empty)

D: (Empty)

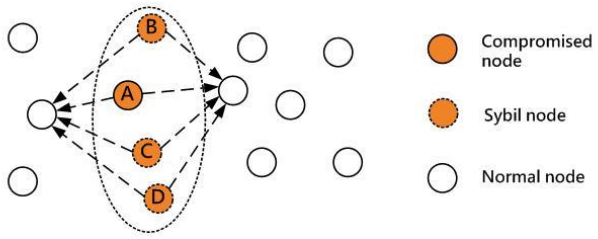

Fig. 3. Sybil Attack

REFERENCES

[1] Joseph Mitola III, Cognitive Radio Architecture, Wiley-Interscience, 2006

[2] Feng Wang, "Cognitive Radio Networks and Security: A Survey" , Journal of Network and Computer Application vol 35, pp. 1691-1708, 2012

[3] Deanna Hlavacek and J. Morris Chang, "A layered Approach to cognitive radio network security:A survey",Computer Networks vol 75 pp. 414-436, 2014

[4] K.–C.Chen,Y.–J.Peng, N.Prasad, Cognitive Radio Network Architecture: Part I – General Structure

[5] Y.C. Hu, Adrian Perrig, David B. Johnson, Packet leashes: a defense against wormhole attacks in wireless networks, in:INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, IEEE Societies, vol. 3, 2003, pp. 1976-1986 (IEEE).

[6] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, A survey of attacks and countermeasures in mobile ad hoc networks, in: Wireless Network Security, Springer, 2007, pp. 103–135.

[7] Chris Karlof, David Wagner,(2003) Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, IEEE.

[8] Dr. Moh. Osama K., (2007),Hello flood counter measure for wireless sensor network, International Journal of Computer Science and Security, volume (2) issue (3)

[9] Cheng-Lung Yang, Wernhuar Tarng, Kuen-Rong Hsieh and Mingteh Chen,"A Security Mechanism for Clustered Wireless Sensor Networks Based on Elliptic Curve Cryptography", Intelligient Internet Systems, issue 33, 2010