Volume 5, Issue 11, November 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Preventing Black Hole Attacks in Wireless Networks

Bala Veeravatnam, D. Suguna Kumari, P. Sowmya
Department of Computer Science & Engineering in Gokaraju Rangaraju Institute of Engineering and Technology, RR Dist, Telengana, India

Abstract: ***In the network environment most of the time there could be more chances of the attacks. That means most of the time does not guarantee about the packets can be easily transfer over the network. It affects network performance degrade. To overcome the above problem of network traffic and performance implementing a Packet Hiding Scheme that can be securely sent packets over the network. While eavesdropping and message injection can be prevented using cryptographic methods, jamming attacks are much harder to counter. They have been shown to actualize severe Denial-of-Service (DoS) attacks against networks. In the simplest form of jamming, the adversary interferes with the reception of messages by transmitting a continuous jamming signal or several short jamming pulses. Typically, jamming attacks have been considered under an external threat model, in which the jammer is not part of the network. In this paper we are developing and surveying on the two schemes that prevent real-time packet classification by combining Cryptographic Puzzles and SHCS. We analyze the security of our methods and evaluate their computational and system overhead.***

Key Terms: Black-hole attack, Routing Protocols, Security, Clustering, Jamming Attacks, AODV.

I. INTRODUCTION

Wireless networks rely on the uninterrupted availability of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it vulnerable to multiple security threats. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones. While eaves-dropping and message injection can be prevented using cryptographic methods, jamming attacks are much harder to counter. They have been shown to actualize severe Denial-of-Service (DoS) attacks against wireless networks. In the simplest form of jamming, the adversary interferes with the reception of messages by transmitting a continuous jamming signal, or several short jamming pulses.

Typically, jamming attacks have been considered under an external threat model, in which the jammer is not part of the network. Under this model, jamming strategies include the continuous or random transmission of high power interference signals. However, adopting an "al-ways-on" strategy has several disadvantages. First, the adversary has to expend a significant amount of energy to jam frequency bands of interest. Second, the continuous presence of unusually high interference levels makes this type of attacks easy to detect conventional anti-jamming techniques extensively on spread-spectrum communications, or some form of jamming evasion (e.g., slow frequency hopping or spatial retreats). Spread-spectrum techniques provide bit-level protection by spreading bits according to a secret pseudo noise code, known only to the communicating parties. These methods can only protect wireless transmissions under the external threat model. Potential disclosure of secrets due to node compromise neutralizes the gains of Spread-spectrum. Broadcast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions. Hence, the compromise of a single receiver is sufficient to reveal relevant cryptographic information.

In our project, we address the problem of jamming under an internal threat model. We consider a sophisticated adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack. The adversary exploits his internal knowledge for launching selective jamming attacks in which specific message s of "high importance" are targeted. For example, a jammer can target route-request/route-reply messages at the routing layer to prevent route discovery, or target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to-end flow.

To launch selective jamming attacks, the adversary must be capable of implementing a "classify-then-jam" strategy before the completion of a wireless transmission. Such strategy can be actualized either by classifying transmitted packets using protocol semantics, or by decoding packets on the fly. In the latter method, the jammer may decode the first few bits of a packet for recovering useful packet identifiers such as packet type, source and destination address. After classification, the adversary must induce a sufficient number of bit errors so that the packet cannot be recovered at the receiver. Selective jamming requires an intimate knowledge of the physical layer, as well as of the specifics of upper layers.

To perform selective jamming, the adversary must be capable of classifying transmitted packets in real time, and corrupting them before the end of their transmission. Packet classification can be performed by receiving just a few bytes of a packet, for example, by decoding the frame control field of a MAC-layer frame. We are interested in developing resource efficient methods for preventing real-time packet classification and hence, mitigating selective jamming

II. SYSTEM ANALYSIS

Problem Statement:

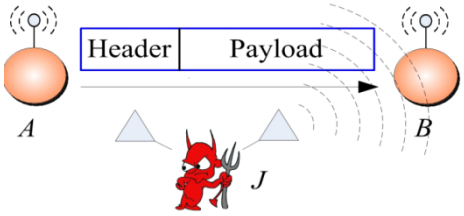

Fig: Selective jamming

Consider the scenario depicted in Figure 1 Nodes A and B communicate via a wireless link. Within the communication range of both A and B, there is a jamming node J. When A transmits a packet m to B, node J classifies m by receiving only the first few bytes of m. J then corrupts m beyond recovery by interfering with its reception at B. We address the problem of preventing the jamming node from classifying m in real time, thus mitigating J's ability to perform selective jamming.

Existing System:

Jamming attacks are much harder to counter and more security problems. They have been shown to actualize severe Denial-of-Service (DoS) attacks against wireless networks. In the simplest form of jamming, the adversary interferes with the reception of messages by transmitting a continuous jamming signal, or several short jamming pulses. Jamming attacks have been considered under an external threat model, in which the jammer is not part of the network. Under this model, jamming strategies include the continuous or random transmission of high power interference signals.

Limitations of Existing System

For instance, delays may be introduced if a multi-hop wireless network is used to route. Furthermore, transmissions in the network must be scheduled carefully information between the plant sensors, actuators and controllers. To avoid packet dropouts due to collisions between neighbouring nodes. These issues can be detrimental to the goal of maintaining stability of the closed loop system if not explicitly accounted for, and substantial research has been devoted to understanding the performance limitations in such settings.

Proposed System

We address the problem of jamming under an internal threat model. We consider a sophisticated adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack. The adversary exploits his internal knowledge for launching selective jamming attacks in which specific messages of "high importance" are targeted. For example, a jammer can target route-request/route-reply messages at the routing layer to prevent route discovery, or target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to-end flow.

To launch selective jamming attacks, the adversary must be capable of implementing a "classify-then-jam" strategy before the completion of a wireless transmission. Such strategy can be actualized either by classifying transmitted packets using protocol semantics, or by decoding packets on the fly. In the latter method, the jammer may decode the first few bits of a packet for recovering useful packet identifiers such as packet type, source and destination address. After classification, the adversary must induce a sufficient number of bit errors so that the packet cannot be recovered at the receiver. Selective jamming requires an intimate knowledge of the physical layer, as well as of the specifics of upper layers.

Network model:

Our network consists of a collection of nodes connected via wireless links. Nodes may communicate directly, or over multiple hops. The nodes of the network can establish globally shared keys, either by manual preload, or via an online key distribution centre.

Adversary Model:

We assume the adversary is in control of the communication medium and can jam messages at any part of the network of his choosing. The adversary can operate in full-duplex mode, thus being able to receive and transmit concurrently. This can be achieved, for example, with the use of multiple radios. In addition, the adversary is equipped with directional antennas that enable the reception of a signal from one node and jamming of the same signal at another. The adversary is assumed to be computationally bounded, although he can be significantly more powerful than the network devices. Solving well-known hard cryptographic problems is assumed to be time-consuming.

III. IMPLEMENTATION

Black Hole:

A black hole has two properties. First, the node exploits the ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting

packets. Second, the node consumes the intercepted packets. We define the following conventions for protocol representation.

Selective Black Hole Attack:

The selective forwarding Attack is sometimes called Gray Hole attack. In a simple form of selective forwarding attack, malicious nodes try to stop the packets in the network by refusing to forward or drop the messages passing through them. There are different forms of selective forwarding attack. In one form of the selective forwarding attack, the malicious node can selectively drops the packets coming from a particular node or a group of nodes. This behaviour causes a DoS attack for that particular node or a group of node.

Distributed and Centralized:

In Distributed based schemes, both sensor node and base stations are responsible for detection and prevention of selective forwarding attack and malicious nodes. On the other hand in centralized based schemes only base station or cluster head are responsible for countering the selective forwarding attack.

Detection and Preventions:

Detection based schemes detect malicious node or the attack or both. On other hand the prevention based schemes only by pass or ignores the malicious node and is not capable of detecting the attack and malicious nodes.

Single Black Hole Attack:

A black hole problem means that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbours. A single black hole attack is easily happened in the mobile ad hoc networks.

Detection, Prevention and Reactive AODV:

An ad-hoc routing protocol is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile adhoc network. Being one of the category of ad-hoc routing protocols, on-demand protocols such as AODV (Ad-hoc On demand Distance Vector) and DSR (Dynamic Source Routing) establish routes between nodes only when they are required to route data packets. AODV is one of the most common ad-hoc routing protocols used for mobile ad-hoc networks. As its name indicates AODV is an on-demand routing protocol that discovers a route only when there is a demand from mobile nodes in the network. In an ad-hoc network that uses AODV as a routing protocol, a mobile node that wishes to communicate with other node first broadcasts an RREQ (Route Request) message to find a fresh route to a desired destination node. This process is called route discovery. Every neighbouring node that receives RREQ broadcast first saves the path the RREQ was transmitted along to its routing table. It subsequently checks its routing table to see if it has a fresh enough route to the destination node provided in the RREQ message. The freshness of a route is indicated by a destination sequence number that is attached to it. Route discovery is a vulnerability of on-demand ad-hoc routing protocols, especially AODV, which an adversary can exploit to perform a black hole attack on mobile ad- hoc networks. A malicious node in the network receiving an RREQ message replies to source nodes by sending a fake RREP message that contains desirable parameters to be chosen for packet delivery to destination nodes. After promising to source nodes that it will forward data, a malicious node starts to drop all the network traffic it receives from source nodes.

An RREP message from a malicious node is the first to arrive at a source node. Hence, a source node updates its routing table for the new route to the particular destination node and discards any RREP message from other neighbouring nodes even from an actual destination node. Once a source node saves a route, it starts sending buffered data packets to a malicious node hoping they will be forwarded to a destination node. Nevertheless, a malicious node drops all data packets rather than forwarding them on.

Black Hole Attack Implementation:

Black Hole node sends the Destination Sequence Number much greater than the Source sequence number to the source node which initiates the route discovery. The sender then sorts the Routing table entries according to the sequence number and starts sending the packets towards the Black hole node. The Black hole node then start drops or alters packets which come from the source or neighbour nodes. The Fixed path or single path has been chosen by the source to send the packets towards the black hole node using modified AODV.

Preventing Black hole using Receive Route Reply (RRR) method:

SN-Source Node
DSN-Destination Sequence Number
SSN-Source Sequence Number
NID-Node ID
MN-ID-Malicious Node ID
RT-Routing Table
SN Broadcasts RREQ
SN Receives RREP


```
SN Stores DSN and NID in RT
Retrieve First entry from RT
IF (DSN>>>=SSN)
    {
        MN-ID=NID
        Black Hole Node
    }
 ELSE
{
        Normal Node
}
```

When the Node with largest Sequence number is received by the source it is considered as a black hole and that route toward that black hole is discarded and the routing table is flushed or updated and sorted according to the destination sequence number.

Propagation of Each information share using Random Dispersive Routing

Randomized multipath routing algorithm that can overcome the fixed path or single path problems. This Algorithm shows that multiple paths will be computed in a random way each time when an information packet needed to be sent to the destination, therefore the number of routes selected by different shares of different packets changing. The randomly generated routes are as dispersive as possible.

SCREEN SHOTS

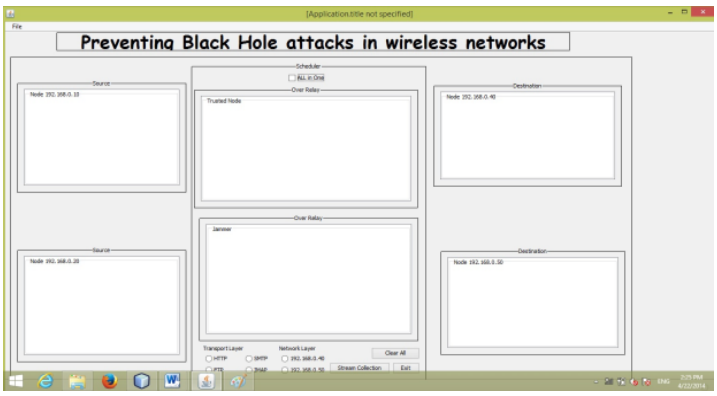

Fig: Screen shot for output screen

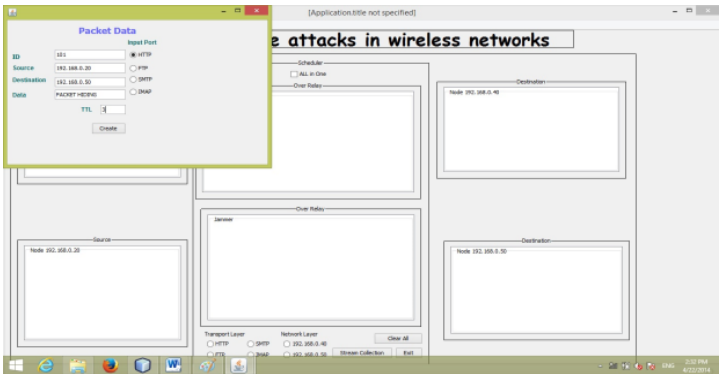

Fig: Screen shot to insert new packet data

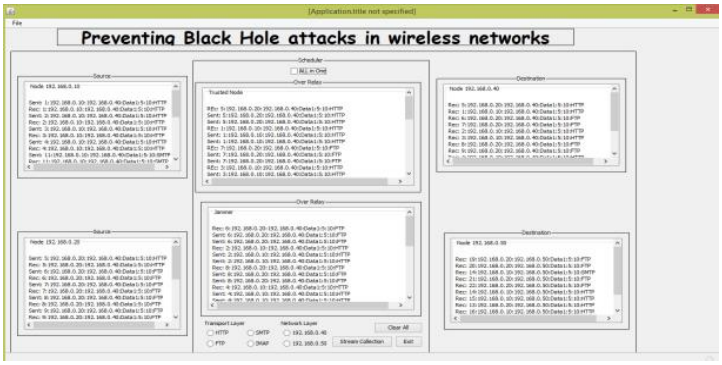

Fig: Screen shot for ordinary transmission of packets

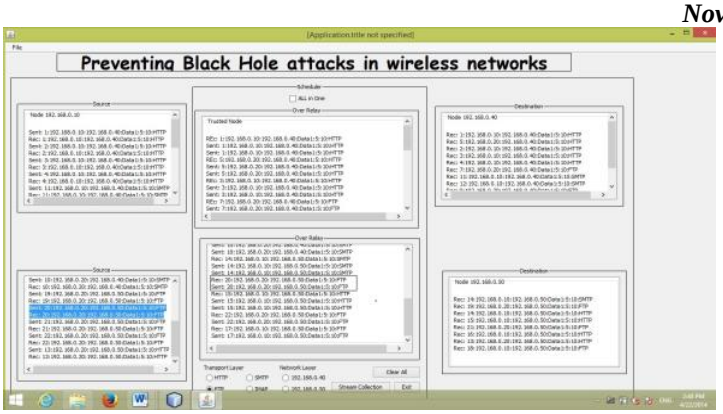

Fig: Screen shot for selective jamming using FTP protocol

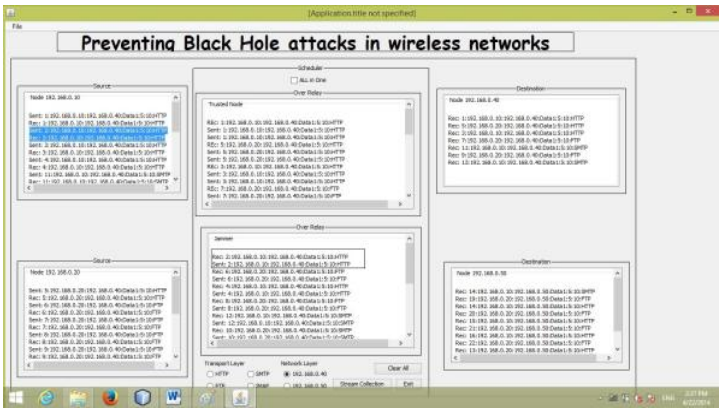

Fig: Screen shot for selective jamming using network layer

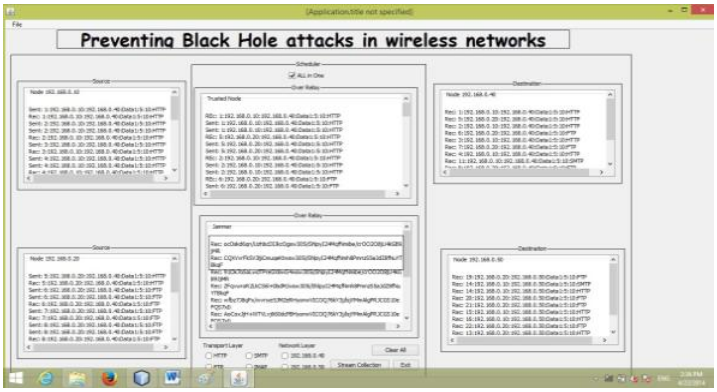

Fig: Screen shot for encrypted mode of transmission

IV. CONCLUSION

We addressed the problem of selective jamming attacks in wireless networks. We considered an internal adversary model in which the jammer is part of the network under attack, thus being aware of the protocol specifications and shared network secrets. We showed that the jammer can classify transmitted packets in real time by decoding the first few symbols of an on-going transmission. We evaluated the impact of selective jamming attacks on network protocols such as TCP and routing. Our findings show that a selective jammer can significantly impact performance with very low effort. We developed three schemes that transform a selective jammer to a random one by preventing real-time packet classification. Our schemes combine cryptographic primitives such as commitment schemes and cryptographic puzzles with physical layer characteristics. We analysed the security of our schemes and quantified their computational and communication overhead.

We have proposed two solutions for the black hole problem. Here, we have studied only one node attack to be in the route (not a group of attackers). The group attack for this problem should be studied.

REFERENCES

[1] Lalit Himral, vishal Vig "Preventing AODV Routing Protocol from Black Hole Attack." International Journal of engineering Science and Technology, Vol3 No.5, May2011, pp 3927-3932

[2] T. Claveirole, M. D. de Amorim, M. Abdalla, and Y. Viniotis. Securing wireless sensor networks against aggregator compromises. IEEE Communications Magazine, pp 134–141, Apr. 2008.

[3] Payal N. Raj and Prashant B. Swadas, "DPRAODV: A dynamic learning system against black hole attack in AODV based MANET", International Journal of Computer Science Issues (IJCSI), Volume 2, Number 3, 2009, pp 54-59.
[4] Lidong zhou, Zygmunt J. Haas, "Securing Ad Hoc Networks", IEEE network, special issue on network security, Vol.13, no.6, November/December 1999.
[5] Yi-Chun Hu, Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy, 1540-7993/04/$20.00 © 2004 IEEE, May/June 2004.
[6] Yih-Chun, Adrian Perrig, David B. Johnson, "Ariadne: A secure On-Demand Routing Protocol for Ad HocNetworks",
[7] A. Al Hanbali, E. Altman, and P. Nain. A survey of tcp over ad hoc networks. IEEE Communications Surveys & Tutorials, 7(3):22–36, 2005.
[8] A. Chan, X. Liu, G. Noubir, and B. Thapa. Control channel jamming: Resilience and identification of traitors. In Proceedings of the IEEE ISIT, 2007.
[10] L. Lazos, S. Liu, and M. Krunz. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In Proceedings of the second ACM conference on wireless network security, pages 169–180, 2009.
[11] R. C. Merkle. Secure communications over insecure channels. Communications of the ACM, 21(4):294–299, 1978.
[12] G. Noubir and G. Lin. Low-power DoS attacks in data wireless LANs and countermeasures. ACM SIGMOBILE Mobile Computing and Communications Review, 7(3):29–30, 2003.
[13] C. Po¨pper, M. Strasser, and S. Cˇ apkun. Jamming-resistant broadcast communication without shared keys. In Proceedings of the USENIX Security Symposium, 2009.
[14] R. Rivest. All-or-nothing encryption and the package transform. Lecture Notes in Computer Science, pages 210–218, 1997.
[15] R. Rivest, A. Shamir, and D. Wagner. Time-lock puzzles and timedrelease crypto. 1996.
[16] M. Abolhasan, T. Wysocki, and E. Dutkiewicz. A review of routing protocols for mobile ad hoc networks. Ad hoc networks, 2(1):1–22, 2004.
[17] C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," in Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99. Second IEEE Workshop on. IEEE, 1999, pp. 90–100.

AUTHOR DETAILS

Mrs Bala Veeravatnam, Post Graduated in Computer Science (M.Tech), JNTUH, 2012, M.C.A From JNTU Hyderabad, 2008. She is working presently as Assistant Professor in Department of Computer Science & Engineering in **Gokaraju Rangaraju Institute of Engineering and Technology**, RR Dist, TS, and INDIA. She has 3 years Experience. Her Research Interests Include Networks, Software Engineering, Cloud Computing, Operating Systems and Information Security.

Mrs D.Suguna Kuamari, Post Graduated in Computer Science (M.Tech), ANU, 2010, and Graduated in Information Technology (B.Tech) From JNTU Hyderabad, 2006. She is working presently as Assistant Professor in Department of Computer Science & Engineering in **Gokaraju Rangaraju Institute of Engineering and Technology**, RR Dist, TS, and INDIA. She has 7+ years Experience. Her Research Interests Include Networks, Software Engineering, Cloud Computing, Operating Systems and Information Security.

Mrs P.Sowmya, Post Graduated in Computer Science (M.Tech), JNTUH, 2014, and Graduated in Information Technology (B.Tech) From JNTU Kakinada, 2012. She is working presently as Assistant Professor in Department of Computer Science & Engineering in **Gokaraju Rangaraju Institute of Engineering and Technology**, RR Dist, A.P, INDIA. She has 1year Experience. Her Research Interests Include Networks, Software Engineering, Cloud Computing, Operating Systems and Information Security.

