Security Considerations in Manets using Cryptography Primitives

[1] Aparna Nimmagadda(mtech), [2] A. Ramana Lakshmi

[1] Student, PVPSIT, KANURU, VIJAYAWADA, KRISHNA DIST.

[2] Associate Prof, PVPSIT, KANURU, VIJAYAWADA, KRISHNA DIST.

Abstract: Adversary disrupts victim's communication channels through jamming in wireless ad hoc network governed by reactive protocols. Attack Models are classified as both internal and external with more strategy employed in external and internal has several disadvantages. Firstly, adversary have to be expand a significant amount energy to frequency bands of interest, and then secondly continuous presence of unusual high interference levels makes the attacks presented for detecting attacks. An internal attack model is an adversary that is assumed to be aware of network secret implementation details of network protocols in any layer present in the network stack. This adversary exploits their internal knowledge for lancing selective jamming attacks in specified messages of high importance are targeted. For this possibility of the selective jamming traditionally used reactive protocols are RREP, RERR, RREQ, RREP are used for primary message format with adversary selective targets in launching of jamming attacks. Prior approaches concentrated on using commitment schemes that are cryptographic primitives to hide the RREQ and RREP packets from the preview of the adversary selective jamming. Prior approaches being successful, we propose to use them along with intrusion detection for identifying compromised routers to increase overall network security significantly by marginalizing the working boundaries of an adversary. Our experimental show efficient implementation validates to users claim data.

Index Terms: Selective jamming, denial-of-service, wireless networks, and packet classification.

I. INTRODUCTION

Wireless network is a type of computer network that uses wireless data connections for connecting network nodes. Wireless networking is a method which homes into telecommunication networks and enterprises installations avoid costly process into a building. In this wireless sensor networks, mobile ad hoc networks is a self configurable networks. In mobile ad hoc network every node randomly moving into appropriate direction from base station other nodes present in network.

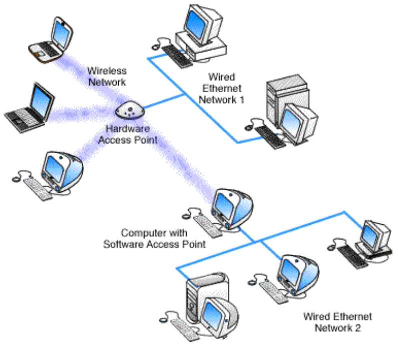


Figure 1: Wireless sensor network architecture.

As shown in the above figure nodes can be moved efficiently and dynamically into other nodes present in mobile ad hoc networks. In this process of network communication jamming is the problem for decreasing network performance with emergency requirement present in mobile ad hoc networks. Jamming is the problem can be occurred in end to end communication/transmission in wireless sensor network. The effects of the jamming at the physical layer resonate through the protocol hierarchy present in wireless sensor network through mobile ad hoc networks.

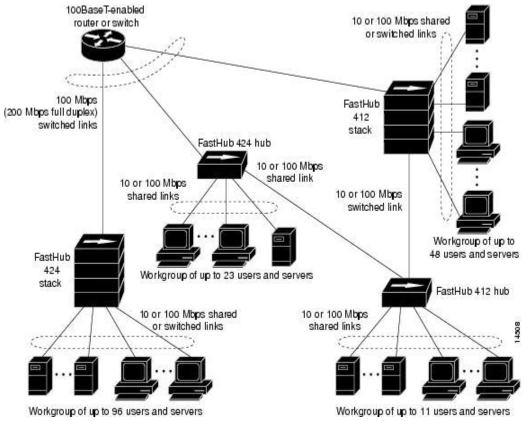

100BaseT-enabled router or switch
10 or 100 Mbps shared or switched links
100 Mbps (200 Mbps full duplex) switched links
FastHub 412 stack
FastHub 424 hub
10 or 100 Mbps shared link
10 or 100 Mbps shared links
10 or 100 Mbps switched link
Workgroup of up to 48 users and servers
FastHub 424 stack
Workgroup of up to 23 users and servers
FastHub 412 hub
10 or 100 Mbps shared or switched links
10 or 100 Mbps shared links
14508
Workgroup of up to 96 users and servers
Workgroup of up to 11 users and servers

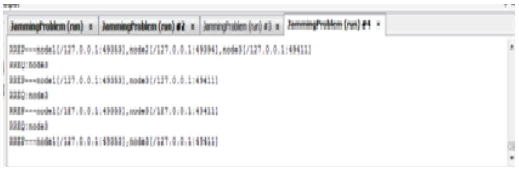
Figure 2: Jamming architecture through routers.

As shown in the above figure the simplest methods were defined for providing anti jamming properties to the wireless sensor networks. Anti jamming methods measures have been into higher layers for data transmission to various channels in mobile ad hoc networks. For example anti jamming protocols may introduce different MAC channels, multiple routing paths for detecting adversary protections form jamming attacks. Traditionally developed security techniques are not suitable data transfer in network with increasing network performance through protocol properties. Packet hiding methods were developed traditionally for application construction with suitable data transfer between every user present in mobile ad hoc networks. But compromised nodes are providing way to abnormal user's identity. So, in this Intrusion and detection were used for identifying compromised routers to increase overall network security significantly by marginalizing the working boundaries of the adversary risking exposure. Due to this to make use of routing diversity, in this achievement each source node must be able to make an intelligent location of traffic across the available paths through the network jamming detection.

II. PROBLEM STATEMENT:

Uses Wireless networks. Packet Types involving in these networks are

1. Route Request (RREQ) Message Format
2. Route Reply (RREP) Message Format
3. Route Error (RERR) Message Format
4. Route Reply Acknowledgment (RREP-ACK) Message Format.



```
RREP---node1[/127.0.0.1:49353],node2[/127.0.0.1:49394],node3[/127.0.0.1:49411]
RREQ:node3
RREP---node1[/127.0.0.1:49353],node3[/127.0.0.1:49411]
RREQ:node3
RREP---node1[/127.0.0.1:49353],node3[/127.0.0.1:49411]
RREQ:node3
RREP---node1[/127.0.0.1:49353],node3[/127.0.0.1:49411]
```

Figure 3: Jamming attack description with attacker node (using Rrep-Ack Rerr, Rrep, Rreq).

Jamming is not a transmit-only activity. It requires an ability to detect and identify the network activity, which denotes in transmitting data in network. As the starting of the network communication present in wireless sensor networks, each layer sensor needs to identify the presence of packet information. In this process packet hiding methods were developed for data transfer in networks. In this achievement packet information can be encrypted through network. And network classifies packets using protocol information. In 802.11 for instance, whether a packet is successfully jammed or not can be seen by whether or not a node sends a short packet (i.e. the RREP-ACK) within 10msec. Typically, jamming attacks have been identified under an external threat exception protocol, in which the jammer is not part of the network. Under this consideration jamming strategies include the continuous/random transmission of high-power interference signal transmission between nodes present in wireless sensor networks. In this model Adversary node can achieve to expand a significant amount of strategy to jam frequency bands of interest, and then continuous to presence of unusual high interference levels makes the type of attacks easy to detect. Conventional anti jamming techniques rely extensively on spread-spectrum (SS) communications, or some form of jamming evasion (e.g., slow frequency hopping, or spatial retreats). Above techniques present bit level protection by spreading bits into secret pseudo noise code to the communication parties. These methods are applicable for only protect wireless transmissions under the external thread model. Fails to efficiently handle internal threat models. So a better jamming detection system is required to handle internal threat models. An efficient comparative schema was developed based on symmetric cryptographic techniques such as AES/DES is used to prevent selective jamming in the wireless sensor networks. A model that employs adversary filtration at the time of network joining though compromised routers is a better way of preventing jamming before it can actually happen. So a better system is required that implements this claim.

III. OUR APPROACH:

Still uses Wireless networks driven by reactive protocols containing RREQ, RREP, RERR, RREP-ACK message packets. Proposes to use commitment schemes along with intrusion detection techniques for identifying compromised routers.

```
Input: Information in the form Packets.

Output: Encrypted data with buffer size
requirements.

Step 1: Appending padding bit of information,
divide message into 64 bits with multiples of 512
bits.

Step 2: Append the length (In binary format
indicating length of the original message into 64
bit)

Step 3: Prepare processing functions like

                    f(t;B,C,D) = (B AND C) OR
((NOT B) AND D)          ( 0 <= t <= 19)
```

f(t;B,C,D) = B XOR C XOR D
(20 <= t <= 39)

f(t;B,C,D) = (B AND C) OR
(B AND D) OR (C AND D) (40 <= t <=59)
f(t;B,C,D) = B XOR C XOR D
(60 <= t <= 79)

Step 4: Prepare processing constants related to original message:

K(t) = 0x5A827999
(0 <= t <= 19)

K(t) = 0x6ED9EBA1
(20 <= t <= 39)

K(t) = 0x8F1BBCDC
(40 <= t <= 59)

K(t) = 0xCA62C1D6
(60 <= t <= 79)

Step 5: Initiate buffers sizes with equivalent constants depending on the number of words:

H0 = 0x67452301

H1 = 0xEFCDAB89

H2 = 0x98BADCFE

H3 = 0x10325476

H4 = 0xC3D2E1F0

Step 6: Processing Message in 512 bit blocks:

K(0), K(1), ..., K(79): 80
Processing Constant Words

H0, H1, H2, H3, H4, H5: 5
Word buffers with initial values.

Figure 3: Secure Hash Function Algorithm for cipher text generation.

As shown in the above figure input message can be converted into cipher text generation using cryptographic features in network communications. By using above sequence we will provide more security considerations based on the process states.

This increases overall network security significantly by marginalizing the working boundaries of an adversary, thus risking exposure. Offers an optimized network performance and security compared to prior systems.

To solve the efficient cryptographic problems are achieved for decreasing the time consuming assurance present in network communications. The most efficient method for deriving the corresponding plaintext is assumed to be an exhaustive search on the key space. Further capable of accessing physical derived network devices and recovery stored information including cryptographic keys and PN codes for data transfer between nodes present in network.

IV. RELATED WORK:

In the previous research, we have studied that the effect of the external selective jammer who targets various control packets in various data links present in the sub layer of data link layer. By using above sequence to perform classification, include to adversary exploits insert in to packet timing information for packet data transfer procedures with transmissions. In [10], Law et al. proposed the estimation of the probability distribution of inter packet transmission times for different packet types based on network traffic analysis. Further data transmission in various layers was predicted using estimated timing information. Using this requirement authors proposed selective jamming strategies for well known sensor network with MAC layer protocols.

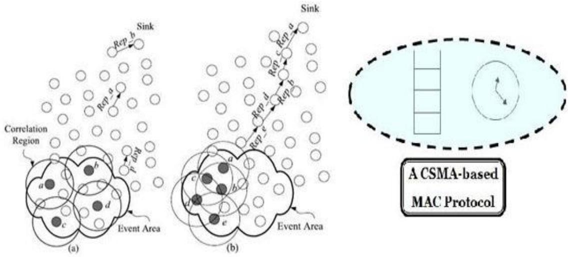


Figure 3: MAC layer protocol efficiency.

Several researchers have been introducing channel selective jamming attacks, in which the jammer targets the broadcast controlling channels. It has shown that shown attacks reduce required power for performing a DoS attack by several orders of magnitude. To control channel accessing that reduces traffic allocated in controlling of transmission.

V. PERFORMANCE ANALYSIS

In this section we describe the efficiency of the network performance into considerable data transmission in mobile ad hoc networks. Construct network with number of nodes using the ip address and port number of the service provider present base station process for transferring data from sender to receiver process. In this we construct Jamming node for data construction with equivalent data transfer between each node present in the mobile ad hoc networks.

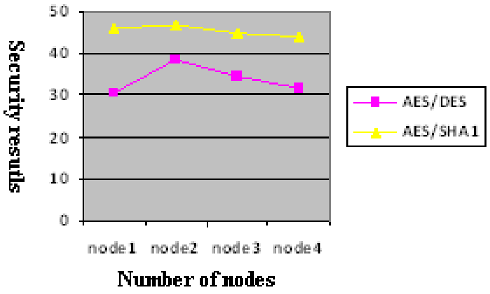


Figure 4: Comparison results with existing and proposed approaches.

As shown in the above figure traditionally used encryption and decryption process for providing security solutions but other nodes are comprised to every node present in the wireless sensor networks. In this paper, we propose to extend our proposed to existing approaches like AES and DES algorithms, to provide efficient security in real time data transfer from service provide to other nodes present in the network.

VI. CONCLUSION:

Wireless network is a type of computer network that uses wireless data connections for connecting network nodes. Attack Models are classified as both internal and external with more strategy employed in external and internal has several disadvantages. Firstly, adversary have to be expand a significant amount energy to frequency bands of interest, and then secondly continuous presence of unusual high interference levels makes the attacks presented for detecting attacks. Prior approaches concentrated on using commitment schemes that are cryptographic primitives to hide the RREQ and RREP packets from the preview of the adversary selective jamming. Prior approaches being successful, we propose to use them along with intrusion detection for identifying compromised routers to increase overall network security significantly by marginalizing the working boundaries of an adversary. Our experimental show efficient implementation validates to users claim data. As further improvement of our proposed work is to provide efficient data transfer in network using advanced algorithms present in the network processing.

VII.REFERENCES

[1] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: A survey," Computer Networks, vol. 47, no. 4, pp. 445–487, Mar. 2005.

[2] E. M. Sozer, M. Stojanovic, and J. G. Proakis, "Underwater acoustic networks," IEEE Journal of Oceanic Engineering, vol. 25, no. 1, pp. 72–83, Jan. 2000.

[3] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems. JohnWiley&Sons, Inc.,2001.

[4] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in Proc. USENIX Security Symposium, Washington, DC, Aug. 2003, pp. 15–28.

[5] D. J. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11b and other networks," in Proc. 25th IEEE Communications Society Military Communications Conference (MILCOM'06), Washington, DC, Oct. 2006, pp. 1–7.

[6] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," IEEE Computer, vol. 35, no. 10, pp. 54–62, Oct. 2002.

[7] G. Lin and G. Noubir, "On link layer denial of service in data wireless LANs," Wireless Communications and Mobile Computing, vol. 5, no. 3, pp. 273–284, May 2005.

[8] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," IEEE Network, vol. 20, no. 3, pp. 41–47, May/Jun. 2006.

[9] D. B. Johnson, D. A. Maltz, and J. Broch, DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks. Addison- Wesley, 2001, ch. 5, pp. 139–172.

[10] E. M. Royer and C. E. Perkins, "Ad hoc on-demand distance vector routing," in Proc. 2nd IEEE Workshop on mobile Computing Systems and Applications (WMCSA'99), New Orleans, LA, USA, Feb. 1999, pp. 90–100.