ISSN 2277-3061

Mitigating Packet Classification for Header Information Retrieval in Wireless Network

Lekshmi.M.R, Prof.N.Nityanandam
Dept of Computer Science and Engg, Archana College of Engineering,Kerala,India
itslekshmihere@gmail.com
Dept of Computer Science and Engg, KCG College of Technology, Tamil Nadu,India
nityanandam.cse@kcgcollege.com

ABSTRACT

Although encryption is used to protect data from being read by unintended recipients it still does not ensure complete safeness. The reason being that information can be gathered by an eavesdropper by indirect inferences like packet classification and traffic analysis. Thus our aim is to protect the header from being read by selective insider jammers. In such a scenario where we have a selective insider jammer who is active only for a period of time, protecting the header information should be given higher priority as these adversaries classify the packets using first few bits from the header fields and add bit errors to the packet if it is an important one. Header information can be protected using modified anonymous routing scheme where we employ multiple level of encryption of the packet to prevent the adversary from classifying the packet using the header information.

Indexing terms/Keywords

Encryption, Adversary, Dependability, Selective jammer, Routing.

Academic Discipline And Sub-Disciplines

Computer Science

SUBJECT CLASSIFICATION

Network security

TYPE (METHOD/APPROACH)

Theory and Experimental Analysis

Council for Innovative Research

Peer Review Research Publishing System

Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

Vol 12, No. 8

editor@cirworld.com

www.cirworld.com, www.ijctonline.com

INTRODUCTION

The major threat to wireless network is Denial of Service attack. An adversary can target on the communication of the nodes and can attempt to create an attack to prevent the efficient communication. In wireless networks such attacks are susceptible from peer nodes. Internal attacks, which are launched from compromised nodes, are more sophisticated in nature. These attacks exploit knowledge of network secrets and protocol semantics to selectively and adaptively target critical network functions. Attack selectivity can be achieved, for example, by overhearing the first few bits of a packet, or classification of transmissions based on protocol semantics. Internal attacks, henceforth referred to as insider attacks , cannot be mitigated using only proactive methods which rely on network secrets, because the attacker already has access to such secrets. They additionally require mechanisms with built-in security measures, through which the attacker can be detected and its selective nature can be neutralized.

Problem Definition

Security and dependability is a prime criterion when we consider exchanging important information between two parties. Even when we employ encryption techniques on payload part, header fields can reveal much critical information that an eavesdropper can gather. When the adversary is an insider compromised node who is aware of the network secrets and protocol semantics, the vulnerability is more. In such a scenario where we have a selective insider jammer who is active only for a period of time, protecting the header information should be given higher priority as these adversaries classify the packets using first few bits from the header fields and add bit errors to the packet if it is an important one. Header information can be protected using modified anonymous routing scheme where we employ multiple level of encryption of the packet to prevent the adversary from classifying the packet using the header information.

Adversary Model

The adversary model considered in this paper is an inside jammer. The adversary can easily launch internal attacks with data alteration, message negligence, selective forwarding, jamming, etc. The insider attackers are severely destructive to the functioning of a network. As the jammer is from within the network, jammer has access to shared cryptographic keys, aware of protocol semantics and the network topologies and may be equipped with advanced hardware like multiple radios, multiple directional antennas and high computational power. The adversary can launch a denial of service attack from within the network. More precisely, the adversary is not only insider but also selective. It targets messages of high importance like control packets. It follows the strategy of smart jamming i.e. “classify-then-jam”. The adversary also has directional antennas which allow reception of signals in one node and jamming the same signal at another node. Furthermore, the adversary can physically compromise network devices and can recover stored information including cryptographic keys, PN codes, etc.

RELATED WORK

The impact of jamming attacks has been focussed under various threat models which include constant jammers, reactive jammers, random jammers and deceptive jammers. In [1,2], Pro˜ano describes the selective jamming attacks in the physical layer. In this, the mitigation strategies include packet hiding schemes which causes considerable communication and computation overhead. In [13], Timothy *X* Brown considers the problem of an attacker disrupting an encrypted victim wireless adhoc network through jamming. This paper address jamming and sensing as two related functions and suggests simple methods for making victim networks less vulnerable to packet classifiers. But roles of multiple attackers were not described and scaling to large adhoc networks were not considered. In [7], L. Lazos address the problem of preventing control-channel DoS attacks manifested in the form of jamming. But the proposed scheme can be utilized only as a temporary solution for re-establishing the control channel until the jammer and the compromised nodes are removed from the network. Fang Liu suggests a novel idea of insider attacker detection in wireless sensor networks [3]. By exploiting the spatial correlation among the networking behaviours of sensors in close proximity, the detection algorithm can achieve high detection accuracy and a low false alarm rate. But the detection algorithm can be specialized by exploring the degree of the correlations existent among different aspects of sensor networking behaviours. This case is not considered in this paper. Various forms of sophisticated attacks launched from adversaries with internal access to the WMN are described by L. Lazos in [6]. These adversaries are detected by aggregate behavioural metrics such as per-packet reputation and credit. However, these metrics cannot detect attacks of selective nature, where only a small fraction of “high value” packets is targeted.

SYSTEM DESIGN AND MODELING

System design defines two scenarios, one in which the real time packet classification takes place and the other which includes the schemes to mitigate the selective jamming attack, which results due to classification of packets in real time.

Real Time Packet Classification

Real time packet classification describes how the adversary can classify the packets in real time, before the packet transmission is completed. When the classification process reveals that the packet has important message, it is easy to jam the packet based on the strategy of the jammer node.

At the physical layer, a packet m is encoded, interleaved and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, deinterleaved and decoded to get the original packet. A packet includes the MAC layer header, IP layer header and TCP layer header. In the MAC layer, the MAC header is removed after processing and the packet is forwarded, then in the IP layer, the IP header is removed after processing and the packet is forwarded and similarly in the TCP layer, the TCP header is removed and the packet is forwarded as shown in Fig 1.

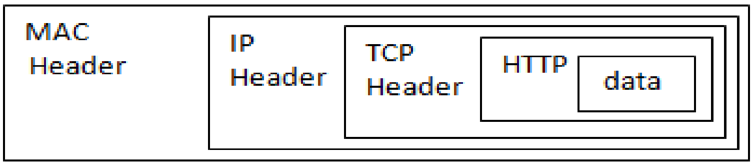
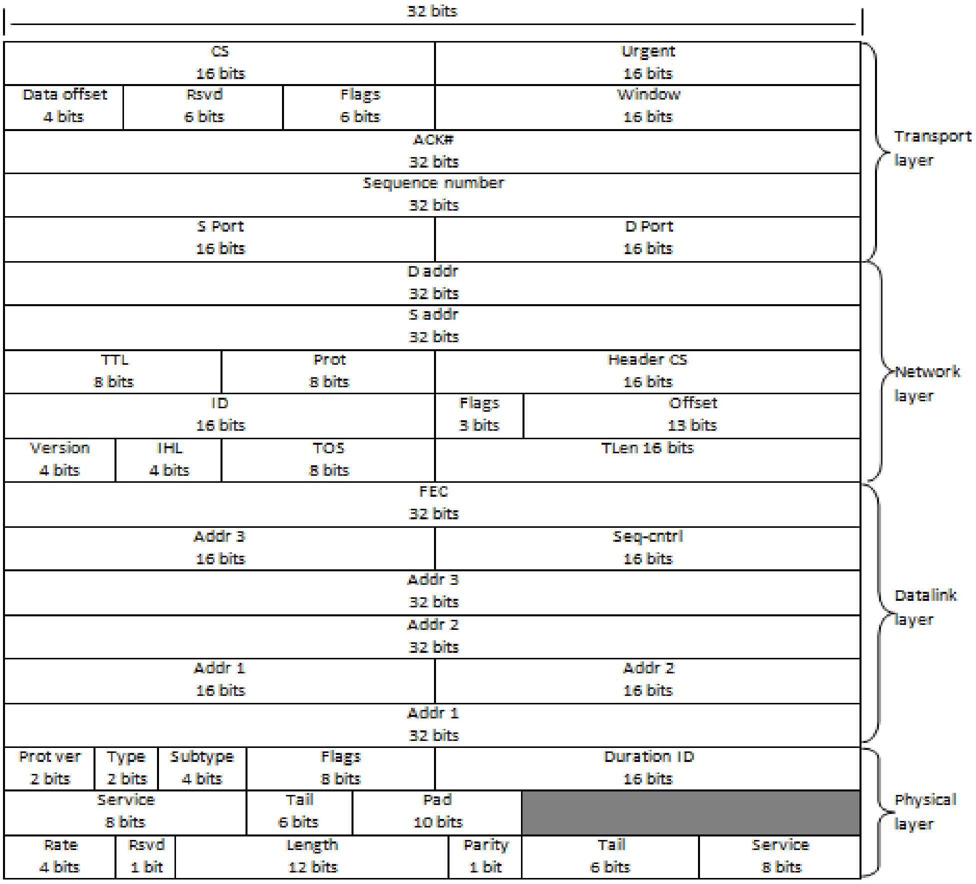


Fig 1 Headers for each layers appended to data

` Physical layer header includes 56 bits. Symbol 1, Symbol 25 and part of Symbol 24 and 2 constitute the physical layer header. MAC layer header includes 224 bits. Symbol 3, Symbol 4, Symbol 5, Symbol 6, Symbol 7, Symbol 8, Symbol 9 and part of Symbol 2, 10 and 24 constitutes the MAC layer header. IP layer header includes 160 bits. Symbol 11, Symbol 12, Symbol 13, Symbol 14, Symbol 15, Symbol 16 and part of Symbol 10 and 17 constitutes the IP layer header. TCP layer header includes 160 bits. Symbol 18, Symbol 19, Symbol 20, Symbol 21, Symbol 22, Symbol 23 and part of Symbol 17 constitutes the TCP layer header. This can be depicted by Fig 2.



32 bits

CS 16 bits	Urgent 16 bits					Transport layer
Data offset 4 bits	Rsvd 6 bits	Flags 6 bits	Window 16 bits			
ACK# 32 bits						
Sequence number 32 bits						
S Port 16 bits	D Port 16 bits					
D addr 32 bits						Network layer
S addr 32 bits						
TTL 8 bits	Prot 8 bits	Header CS 16 bits				
ID 16 bits	Flags 3 bits	Offset 13 bits				
Version 4 bits	IHL 4 bits	TOS 8 bits	TLen 16 bits			
FEC 32 bits						Datalink layer
Addr 3 16 bits	Seq-cntrl 16 bits					
Addr 3 32 bits						
Addr 2 32 bits						
Addr 1 16 bits	Addr 2 16 bits					
Addr 1 32 bits						
Prot ver 2 bits	Type 2 bits	Subtype 4 bits	Flags 8 bits	Duration ID 16 bits		Physical layer
Service 8 bits	Tail 6 bits	Pad 10 bits	▨			
Rate 4 bits	Rsvd 1 bit	Length 12 bits	Parity 1 bit	Tail 6 bits	Service 8 bits	

Fig 2 Header fields for each layer

At the modulator, the output of the interleaver is modulated as 25 OFDM symbols. Here,

1 symbol = 24 bits

25 symbols = 600 bits

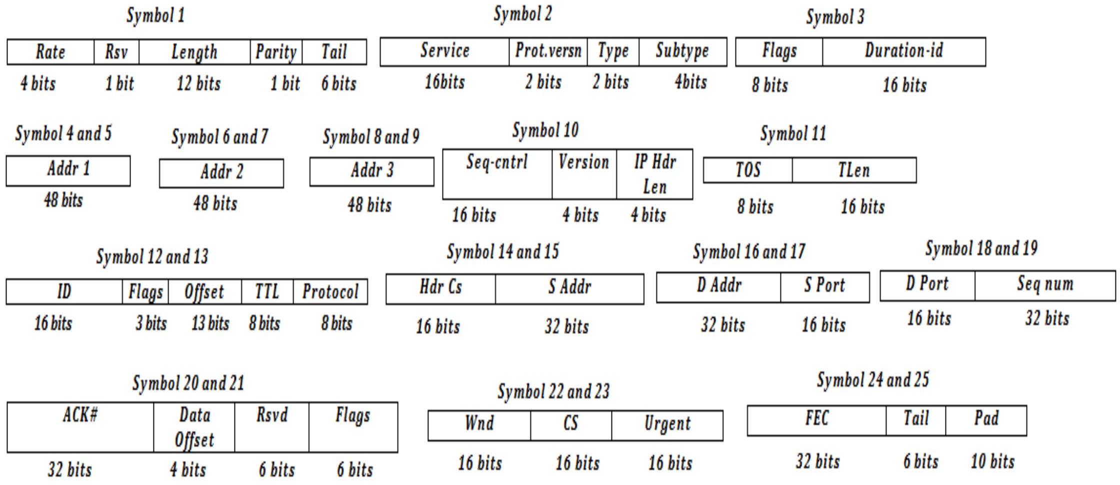


Fig 3 Header Fields grouped as 25 OFDM symbols

Fields in the headers that leads to packet classification

A packet can be classified based on the headers of various layers. For example, the MAC header typically contains information about the type and subtype of MAC frame. The TCP header reveals the end-to-end source and destination nodes, the transport-layer packet type (SYN, ACK, DATA, etc.), and other TCP parameters. Not all the header field can cause classification of a packet. Only certain header fields can reveal whether a packet is having important data or not.

Classification in datalink layer mainly occurs in the symbols, frame type and WEP. Frame type reveals the control information which leads to classification. When the WEP field in Flags is set to 1, it indicates that encryption schemes have been used, leading to classification. Classification in network layer mainly occurs in the symbols, Type Of Service and Option. TOS reveals about the type of service provided. Option reveals about the source routing informations. Classification in transport layer mainly occurs in the symbols, destination port and URG. Destination port reveals about the destination of the respective packet. When the URG is set to 1, it indicates that the packet is important, leading to classification. One of the important fields that lead to classification is header length (IHL). If header length of the entire packet exceeds 600 bits, then it indicates that encryption schemes have been used. This leads to classification.

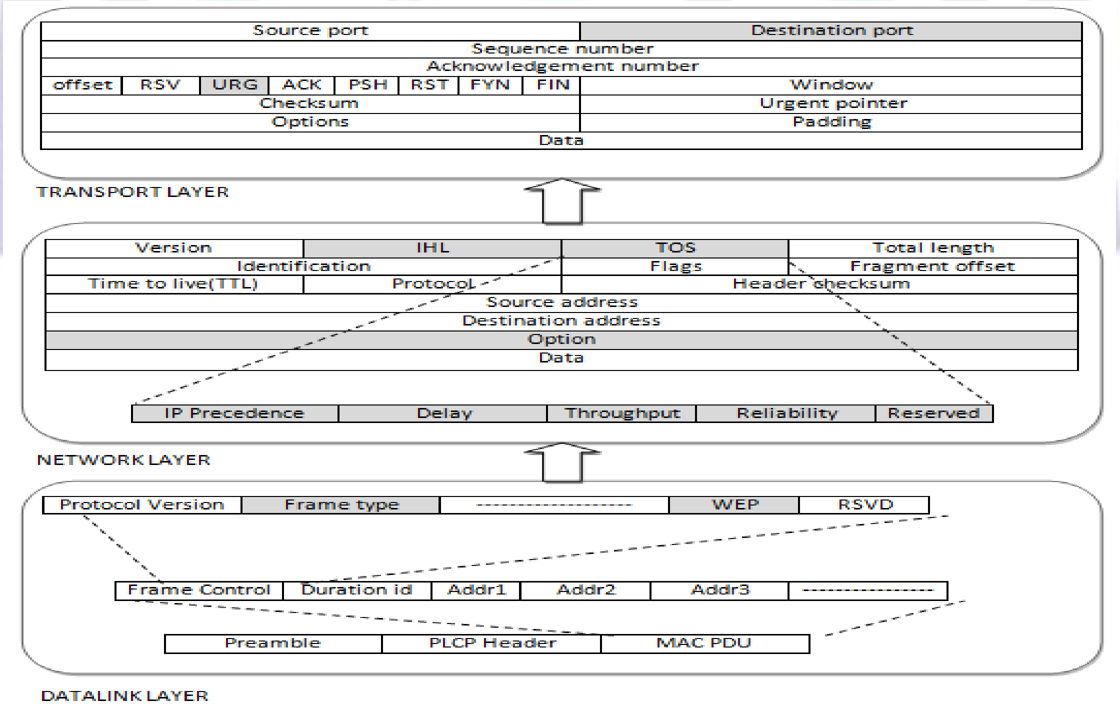


Fig 4 Real time packet classification

Mitigation of Real Time Packet Classification: Modified anonymous routing scheme

Although encryption is used to protect data from being read by unintended recipients it still does not ensure complete safeness. The reason being that information can be gathered by an eavesdropper by indirect inferences like packet classification and traffic analysis. Thus our aim is to protect the header from being read by selective insider jammers, which can be achieved by anonymous routing scheme called onion routing in wireless networks. In onion routing the data is wrapped in layers of encryption in a data structure called as an onion, which is transmitted over the network. The onion is constructed in such a way that it prevents any eavesdropper from gaining information about the parties involved in the communication or the nature of their data exchange.

Onion Routing

Onion routing is the mechanism in which the sender and the receiver nodes communicate with each other anonymously by means of some anonymous intermediate nodes called as onion routers. It protects against traffic analysis and makes it very hard for an eavesdropper to determine who is talking to whom over the network. It concentrates on encrypting the packet header in such a way that only the intended destination understands that the packet is meant for him. Onion refers to the transmission data wrapped in multiple layers of encryption with the route information in each layer of encryption. It is done in such a way that when the data moves from one onion router to the next, each onion router strips a layer of the onion using its private key to find its next hop, and routes the packet accordingly.This goes on till the packet reaches the receiver. Thus every onion router knows only its previous and next hop. Padding may be applied at each onion router to maintain the size of the onion. So data passed along this anonymous connection appears different to each onion router. Also since an onion is decrypted at each router there is no correspondence between an incoming and outgoing onion for a particular router. Hence data cannot be tracked in route and even a compromised onion router cannot be of much help. Even if an onion router is compromised only the previous and next hop would be visible but the actual sender and receiver would still be hidden. This provides added resistance to an attacker. Since the size of the onion reduces as it nears the destination an attacker can infer details about the destination. To avoid this onions are padded at each onion router to maintain the size of the onion. Padding is simply adding redundancy. This is a really big advantage because it complicates traffic analysis, as an attacker cannot infer location or other details of the destination by getting hold of an onion. Every onion router has details of only its previous and next hop. So even if an onion router has been compromised the attacker can only get the encrypted onion with the next hop. He will not be able to decrypt the onion without the private keys and hence will not infer any valuable information from it.

Algorithm

The basic anonymous routing scheme is based on the concept of onion routing. It is divided into 3 phases; route discovery, route reply and data forwarding. This protocol makes a few assumptions as follows:

- Every node in the network has a permanent identity known to all other nodes in the network.
- The source and destination share a secret key KSD.
- Nodes share secret keys only with a limited set of other nodes.
- Every node establishes a broadcast key with its one hop neighbourhood.

The basic anonymous routing protocol has been modified to create a modified anonymous routing scheme, which has been applied as the mitigation scheme. The algorithm is as follows,

Source: S

Targeted destination: D

Sequence number: SN

Destination identifier and key: DIK

Initial value of ttl field: ttl_{init}

Asymmetric key pair: AKP1, AKP2

Encrypted link identifiers: $E_{AKP1}(n_S; k_S)$

Route Discovery:

At source node S;

1) S generates asymmetric key pair AKP1 and AKP2.

2) S generates Destination identifier and key (DIK) that can only be opened by node D that has knowledge about the Ksd.

DIK : E_{Ksd} (D,S,AKP2,ttl_{init})

3) S also generates random pair of link identifiers (n_s,k_s) ,used to recognize RREP messages.

4) S encrypts the pair of link identifiers using AKP1

5) Finally the packet is broadcasted by S.

S→* : D; S; ttl_{init} ; AKP1; DIK; $E_{AKP1}(n_s, k_s)$,SN

At receiving node N_i;

1) Checks whether it is the targeted destination of the RREQ by verifying destination id, D.

2) If so, N_i tries to decrypt the DIK to check whether the first part of the DIK id matches with its own id. If it doesn't match, N_i is not the targeted destination.

3) If N_i is not the targeted destination, node checks whether SN has been recorded in the routing table. If it is recorded then discard the RREQ message. Else N_i stores it in the routing table.

N_i stores in routing table: D, S, n_{i-1}, k_{i-1}, SN

4) If ttl>1, decrement ttl and encrypt the link identifiers as onion using AKP1 and append this to the broadcast message. If ttl=0 then discard the packet.

N_i →* : D, S, ttl ,AKP_1, DIK; E_{AKP1} (……..(E_{AKP1} (n_{i-1}; k_{i-1}),n_i,k_i))

5) When N_i is the targeted destination, it stores the complete RREQ in memory and it decrypts DIK to get ttl_{init}, AKP2. It uses AKP2 to get link identifiers of all the intermediate nodes.

6) Compute the number of hops to select the shortest route, h=ttl- ttl_{init} and generate n+1 link keys, S_i

7) Construct a reply onion which contains link ids of all intermediate nodes and encrypt them several times using ids of intermediate nodes in reverse order. set the ttl value as h+1.

8) Unicast this route reply as E_{kD}(S;ttl); E_{kn}(n_n,s_n,s_{n-1}, E_{kn-1}(n_{n-1},s_{n-1},s_{n-2},…….., E_{ks}(n_s, s_s))),n_n

Route Reply:

At the destination D;

1) D generates n+1 link keys S_i for $0 \le i \le n$ where $s_0 = s_{source}$. Link key will be shared between N_i and N_{i+1}.

2)The onion can be generated as O_n = E_{kn}(n_n,s_n,s_{n-1}, E_{kn-1}(n_{n-1},s_{n-1},s_{n-2},…….., E_{ks}(n_s, s_s)))

3) Unicast this route reply as E_{kD}(S;ttl); O_n,n_n. The identifier and ttl field of RREP are encrypted with the current unicast key to hide them from insider adversaries.

At the receiving node N_i,

1) Node N_i strips one layer of the onion, decrement ttl value and encrypt the new header with N_i's previous hop key (if it is not indented receiver).

2) If ttl>1, decrement the ttl and stores the secret keys (s_i,s_{i-1}) and previous hop. Forward the packet to the next hop. if ttl=0, discard the packet.

3) If the id matches with that of id S, then it is the intended recipient. Strip the onion to get the intended message

4) Finally initiate the process of data forwarding.

Data Forwarding:

1) Data messages will have the same format as RREQ packets.

S→* : D; S; ttl_{init} ; AKP_1; E_{Ksd} (D,S,AKP_2,ttl_{init} ,M); E_{AKP1}(n_S, k_S) ,SN

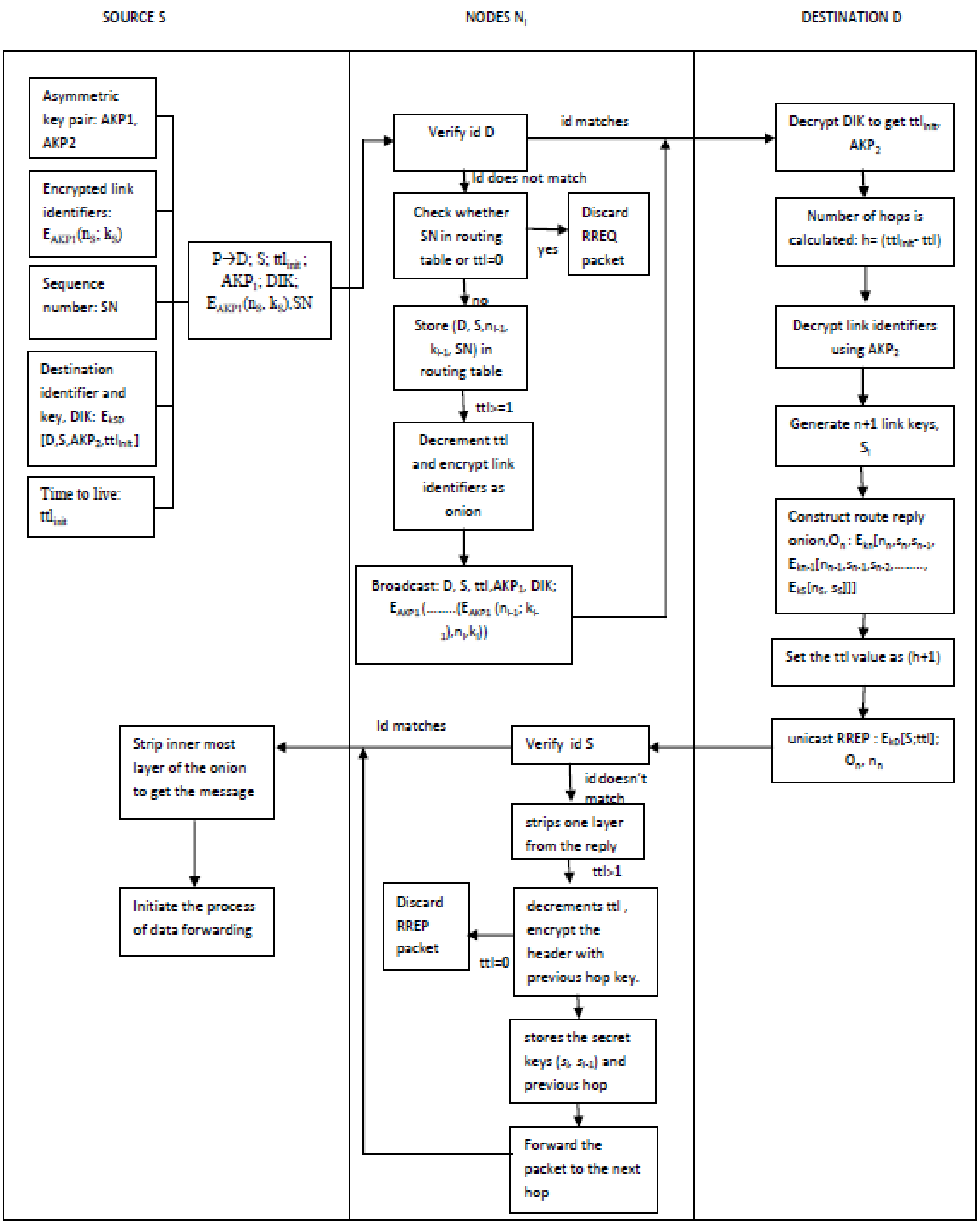

SOURCE S
NODES N_i
DESTINATION D
Asymmetric key pair: AKP1, AKP2
Encrypted link identifiers: E_AKP1(n_S; k_S)
Sequence number: SN
Destination identifier and key, DIK: E_kSD [D,S,AKP_2,ttl_init]
Time to live: ttl_init
P→D; S; ttl_init ; AKP_1; DIK; E_AKP1(n_S, k_S),SN
Verify id D
id matches
Id does not match
Check whether SN in routing table or ttl=0
yes
Discard RREQ packet
no
Store (D, S,n_i-1, k_i-1, SN) in routing table
ttl>=1
Decrement ttl and encrypt link identifiers as onion
Broadcast: D, S, ttl,AKP_1, DIK; E_AKP1 (--------(E_AKP1 (n_i-1; k_i-1),n_i,k_i))
Decrypt DIK to get ttl_init, AKP_2
Number of hops is calculated: h= (ttl_init- ttl)
Decrypt link identifiers using AKP_2
Generate n+1 link keys, S_i
Construct route reply onion,O_n : E_kn[n_n,s_n,s_n-1, E_kn-1[n_n-1,s_n-1,s_n-2,--------, E_kS[n_S, s_S]]]
Set the ttl value as (h+1)
unicast RREP : E_kD[S;ttl]; O_n, n_n
Id matches
Verify id S
id doesn't match
strips one layer from the reply
ttl>1
decrements ttl , encrypt the header with previous hop key.
ttl=0
Discard RREP packet
stores the secret keys (s_i, s_i-1) and previous hop
Forward the packet to the next hop
Strip inner most layer of the onion to get the message
Initiate the process of data forwarding

Fig 5 Architecture for mitigation scheme

RESULT AND ANALYSIS

Simulation results enable the evaluation of the network performance with respect to the network density/ number of nodes. It explains the network performance with respect to the attacks caused by the selective jammer as a result of packet classification. Xgraph is a plotting program in ns-allinone package which can be used to create graphic representations of simulation results. The output files in the Tcl scripts are used as the data sets for xgraph.

In this scenario, 24 nodes are taken and placed in different positions with flat grid topology of which 15 nodes take part in the transmission of data. Continuous Bit Rate traffic sources are used for traffic model. Finish time of the simulation is set to 2ms. Omni antenna model is used. Size of the topography is set to 980 for the x axis and 1640 for the y axis. Number of nodes refers to the network density. In this system there are 24 nodes in the network of which 15 nodes are involved in the packet transmission. The group size of the topology is 4 and the number of nodes per group is 6. Thus the total number of nodes in the topology is 24.

Simulation has been done for 2ms.The time taken for real time packet classification in the presence of a selective jammer at different position has been analysed in the initial stage. In the next stage, modified anonymous routing scheme has been applied as a mitigation scheme for preventing the selective jammer from classifying the packet. Then the time taken for real time packet classification with the mitigation scheme has been analysed. Graph was generated for both the cases and the graphs were compared to analyse the efficiency of the proposed scheme. The average throughput for the existing and proposed system has also been computed to analyse the impact of the mitigation scheme.

Time taken for real time packet classification with and without the mitigation scheme

A selective jammer jams a packet by reading the header information and then by classifying the packet into important and unimportant packets where the important packets are jammed. With the mitigation scheme, the jammer takes considerable time for classification and thereby the jammer is delayed in real time packet classification. Without the mitigation scheme, the average time taken by a selective jammer for real time packet classification ranges from 3.4451ms to 3.89893ms. With the mitigation scheme, the average time taken by a selective jammer for real time packet classification ranges from 4.60105ms to 4.95877ms. This clearly depicts that the packet would reach the destination before the jammer could classify the packet.

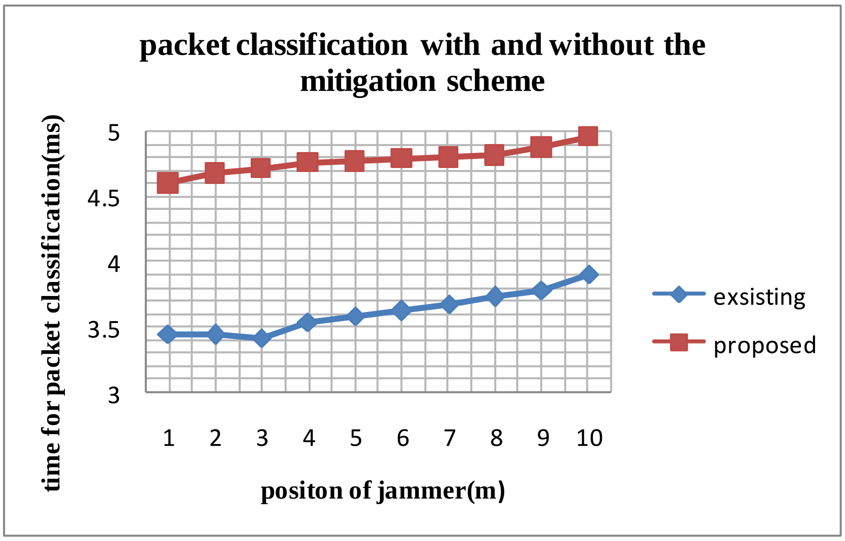


Fig 6 Time for packet classification vs position of jammer

Average Throughput analysis with and without the mitigation scheme

Average throughput can be defined as the average number of packets transmitted per unit time. It is the average rate of successful message delivery over a communication channel. The graph in Fig 7 depicts the average throughput with and without the mitigation scheme. The throughput drops drastically in the presence of a selective jamming attack. The throughput is approximately 79% in the existing system which has been increased to 92% by applying the modified anonymous routing scheme .In the existing system, the average throughput is less in the presence of a selective jammer. In the proposed system, the jammers ability to classify the packet has been alleviated using modified anonymous routing scheme which leads in the increase of throughput to 92 %.

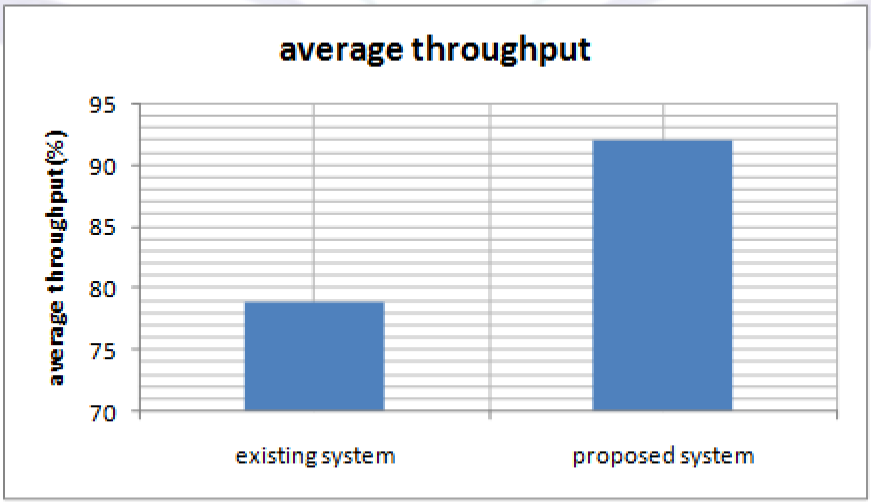


Fig 7 Average throughput comparison in existing and proposed system

CONCLUSION

Wireless networks are prone to various external and internal security threats. While most external attacks can be mitigated easily, internal attacks are much harder to counter because the adversary is aware of the network secrets and its protocols. Creating broadcast communication with jamming resistant environment in the presence of inside jammers remains a challenging problem. Using cryptographic techniques of encrypting both header and payload can prevent jamming to a certain extent. But cryptographic keys can be easily exposed in the event of node compromise. However, the enhanced level of security comes at the expense of performance, because broadcasted messages have to be transmitted multiple times and on multiple frequency bands to guarantee robust reception. Moreover, even if packet reception of critical messages is ensured, inside adversaries are in complete control of the traffic routed through them. A selective inside jammer can impart both data selective jamming and control channel selective jamming. Most existing methods assume a continuously active adversary that systematically drops or add bit errors to the packets. These adversaries are detected by aggregate behavioural metrics such as per-packet reputation and credit. However, these metrics cannot detect attacks of selective nature, where only a small fraction of "highly important" packets is targeted. Furthermore, when the adversary drops only a few packets, his behaviour can be indistinguishable from dropping patterns due to congestion or poor wireless conditions.

In such cases, a clear evaluation has to be done to understand how real time packet classification is done by a compromised node to identify the packet as a highly important one. In this paper, various header informations that reveal the importance of the message have been studied and a scheme has been proposed to prevent the real time packet classification of the packet during transit. Simulation results are based on the network performance with respect to the network density. Finally the conclusions made are,

- ✓ How the adversary classified packets in real time.
- ✓ Illustrated the impact of selective jamming attacks on the network performance.
- ✓ How packet classification can be mitigated through delaying scheme.
- ✓ Evaluation of the delaying of packet classification scheme is done.

REFERENCES

[1] A. Pro˜ano and L. Lazos, Packet-Hiding Methods for Preventing Selective Jamming Attacks, IEEE Transactions on Dependable and Secure Computing, Vol. 9, pp. 101–114, 2012.

[2] A. Pro˜ano and L. Lazos, Selective Jamming Attacks in Wireless Networks, IEEE International Conference on Communications (ICC), pp. 1–6, 2010.

[3] Fang Liu and Xiuzhen Cheng, Insider Attacker Detection in Wireless Sensor Networks, 26th IEEE International Conference on Computer Communications, IEEE INFOCOM, 2007.

[4] Kemal Bicakci and Bulent Tavli, Denial-of-Service attacks and counter measures in IEEE 802.11 wireless networks, Elsevier Journal on Computer Standards and Interfaces.

[5] M. R. Lekshmi and Nityanandam N., Effectual strategies to Thwart Selective Jamming Attacks in Wireless Network, 2nd International Conference on Emerging Marvels in Information and computer Science and Engineering, 2013.

[6] L. Lazos and M. Krunz, Selective Jamming/Dropping Insider Attacks in Wireless Mesh Networks, IEEE Network, Vol. 25, No. 1, pp. 30–34, 2011.

[7] L. Lazos, S. Liu and M. Krunz, Mitigating Control Channel Attacks in Multi-channel Ad-Hoc Networks, 2nd ACM Conference on Wireless Network Security (WiSec), 2009.

[8] L. Lazos, S. Liu and M. Krunz, Thwarting Inside Jamming Attacks on Wireless Broadcast Communications 4th ACM Conference on Wireless Network Security (WiSec), 2011.

[9] Payal Jain and Sameer Verma, Study and Analysis of security Issues inWireless Sensor Network, Global Journal of Computer Science and Technology, vol. 11, issue 16, 2011.

[10] S. Liu, L. Lazos and Marwan Krunz, Jamming-resistant Broadcast Communications under Internal Threats, IEEE Transactions on Mobile Computing (TMC), p. 14, February 2012.

[11] W. Stallings, Wireless Communications and Networks, 2nd Edition, Prentice Hall, 2005.

[12] S. Liu, L. Lazos and M. Krunz, Thwarting Control-Channel Jamming Attacks from Inside Jammers, IEEE Transactions on Mobile Computing (TMC), DOI: 10.1109/ TMC.2011.165.

[13] Timothy X. Brown, Jesse E. James and Amita Sethi, Jamming and Sensing of Encrypted Wireless Ad Hoc Networks, MobiHoc'06 Conference.

[14] C. K. Toh, Adhoc mobile wireless networks-protocols and systems, Pearson Education Publications, ISBN 978-81-317-1510-9.

Author' biography with Photo

Prof N Nityanandam is currently working as Professor in the department of Computer Science and Engineering at KCG College of Technology, Chennai, India. Before moving to Academics he worked as a Scientist in a Naval R&D at Cochin, India and he was a Wing Commander in India Air Force in the Directorate of Information Technology. He did his masters degree in computers from IIT, Kanpur, India and Bachelors degree from College of Engineering, Guindy, Madras, India. His Areas of interest are Network Security, Mobile and Wireless Networks.

Lekshmi.M.R is currently working as Assistant Professor, in Computer Science and Engineering Department, Archana College of Engineering,Kerala,India. She obtained her masters degree from KCG College of Technology,Chennai in 2013 and bachelors degree from The Rajaas Engineering College,TamilNadu,India . Her areas of interest include Network Security, Web Engineering, Software Engineering.