Chapter 2

Literature Survey and Background study

2.1 Introduction

In wireless communication the network is well established & secured under various communications. But in the current scenario due to advancements in Technology we are facing some problems as well. Nodes are connected to the network and communicate with other nodes within or outside the network. During the communication the Routing methods set the nodes to be a part of communications to connect, send & receive the Packets. In the wireless network the some adversaries outside the node doesn’t allow the users to make secure communication. Such External threats can be effective when they perform Packet Dropping, Channel Jamming and Buffer Overflow etc.

Sometimes the nodes already in the network change their nature and become adversary node in the network. In addition to this they interrupt the communication occurs in the network. Some internal fellow contestant nodes possessing knowledge of protocol specification and network secrets can perform jamming attacks with low-effort that are hard to detect. (JOSHNA, S et al., 2013)

An article by Justin & Raj represents that Selective jamming attacks requires real time packet classification at the physical layer. In addition to this to perform the attack Constant Jammer is used at the physical layer. There are other three types of link layer jammer known as deceptive, random, and reactive jammer. The reactive Jammer is the most sophisticated as it is smart enough to launch attack after identifying the process of Transmission. The jammer will identify activity being done currently in the network. This will enable the attacker to control its resources for performing attacks without wastage. (JUSTIN et al., 2012)
Additionally prior sensing of network activity enables attacker to keep its identity hidden until necessary attack is being performed. The jammer sends noise to the channel of legitimate packet stream. As a result of such action, collision of the packets occurs at receiver end. This whole activity degrades PDR and interrupts communication. (JUSTIN et al., 2012) “How the node can identify that a particular node is a jammer?” The answer for this question is that a node which receives repeated acknowledgements for the same message or another situation is that the packet is held by a node in the network for a long time (not because of high network traffic) or if any node that violates the rules in a particular network region. Then the access point can identify that the particular node is a jammer. (LUKE, Divya Ann and S., Dr.Jaysudha J., 2014)

Here an adversary model is built with nodes (attackers) which have enough information regarding their target network and protocols. Also they launch selective jamming attack targeting “high importance” packets with the help of this knowledge. To perform jamming activity adverse nodes remains active for small period of time. In addition to this jammer is also capable of performing classification of transmitted packets in real time. Jammer performs selective jamming instead of continuous jamming as continuous jamming wastes energy and other resources. Also with selective jamming they can corrupt the packets before end of transmission. In addition to this, the jammer must be capable of implementing a “classify-then-jam” policy before the completion of a wireless transmission. Jamming attacks are much harder to solve and more security problems. (M, Abhimanyu V and L, n.d., 2012)

Packet Classification can be done by receiving the packet partially as decoding the control field of MAC layer frame. So resource efficient methods are being developed to overcome real-time packet classification and preventing selective jamming. (ALEJANDRO, Proano and L, L, 2011)

We investigate the feasibility of real-time packet classification for launching selective jamming attacks. We consider a sophisticated adversary
who exploits his knowledge on network protocols along with secrets extracted from compromised nodes to maximize the impact of his attack. (WENYUAN, Xu and W, T, 2005)

Due to the internal threat model here it is very tough to identify the adverse nodes. Also to identify such activity we need to understand the unorthodox behaviour of the nodes. Also some exception cases of network model failures or node failures must have to be considered as authentic failure instead of attack. We have to make a system which works at physical layer and provides enough security to overcome the Real Time classification. So even in the case of Internal Threat Model the adverse nodes are unable to perform Classification and Jamming based on it. The Packets are to be made enough secured and transmitted through route decided by the Routing algorithm on wireless channel.

2.2 Attacks in Wireless Network

WLAN technology provides mobility and wireless connectivity and is now part of day to day life. WLAN technology and architecture is presented by Gast and Mark in 2005. WSN uses DNS hierarchical tree structure to represents node in network. Raymond and Midkiff did research on DoS attacks in WSN in 2008. Varadarajan, Kumar and Reddy made experiments regarding improving network performance and DoS attacks in 2011. Due to open nature of wireless network, any transceiver in wireless network can eavesdrop on transmission, inject spurious messages or jam the target node. Security in any type of wireless network is a challenging issue. Security in WLAN is provided by encryption and authentication (P, RameshKumar et al., 2013). Most of the existing jamming techniques in WLAN use external threat model. In this threat model jammer node is not the part of network. So, it is easy to attack in wireless network and jam the network by identifying the specific channel of communication between the nodes. Messages of target node are blocked by jammer node. Wireless networks are more sensible to DoS attacks (LUKE,
Divya Ann and S., Dr.Jaysudha J., 2014) Spread Spectrum is used for communication in WLAN. To prevent the external threat in WLAN, security is provided by a method in which Psudo noise code (PN code) is adding to signal which will encode the signal and protect the channel from jamming attack. This code is known to both communicating parties and protects the network from the external jammer node. Jammer node can change the channel and attack on the network (WOOD, Anthony and Stankovic, John A., 2002). A selective Jamming attack in Wireless network is a passive attack and is done by jammer in internal threat model. In internal threat model jammer node is a part of WLAN and has an internal knowledge of network and has detailed configuration of network. So it is very difficult to detect jammer node. Worm hole based anti-jamming method SHCS (PROAN˜O A, Lazos L, 2012) is proposed to mitigate selective jamming attack in wireless network. It also improves network performance by implementing shortest path method. Permutation and AES encryption is used to hide the packet for the security purpose. Prevention of Selective Jamming (ASHISH KUMAR et al., 2013) method is based on classification of transmitting packets using protocol stack semantics (S., Periyanayagi and V., Sumathi, 2011), decoding packets during transmission or decode first few bits of packet at physical layer during real time transmission and add noise so that receiver node cannot receive packets (LAW Y W, Palaniswami M, Hoesel L V, Doumen J, Hartel P, Havinga P, 2009). Selective Jamming attacker requires knowledge of Physical layer and also all above layers. AONT-HS is proposed to prevent selective jamming by using padding function with original message using encryption algorithm to all parts of messages (P, RameshKumar et al., 2013). Swarm based intelligent method is used in WSN to implement AONT-HS. Cryptographic Puzzle is also used for active jammer attack. Here sender node sends encoded packets by implementing cryptographic puzzle and only receiver knows the results. If attacker tries to capture the packets and decode but due to not having a proper key, time is wasted and packet drops. Jammer is active during whole transmission and its energy is wasted quickly due to low battery life. Multi hop
WSN is also facing issue of radio jamming, by using Honeypot technique (S. S., Justin Raj and D., Thilagavathy, 2012) in which multiple channels and implementing monitor nodes to monitor activities of jammer node, it is easy to switch on new frequency. Monitor nodes pass notification to other node regarding activities of jammer nodes in WSN. Jamming characteristic and metrics are discussed and importance of PDR, PLR and PSR is to be highlighted to develop and design anti-jamming algorithm (WENYUAN, Xu and W, T, 2005). Signal strength, carrier sensing time and PDR is used to detect various jammers with the jamming model of constant jammer (continuously emits signals), reactive jammer (jams only when any transmission occurs), deceptive jammer (continuously sends fabricated messages or replays old ones) and random jammer (acts periodically). All these models of jammer (PROAN˘O A, Lazos L, 2012) are tested with TCP protocol by using cryptographic primitives to mitigate jamming attacks. Jamming attacks prevention in WSN by using secure packet hiding by adding hidden sub layer (SEKHAR, J. C. et al., 2013) is added between physical layer and MAC layer by using cryptographic primitives SHCS, CPHS,AONT-HS. In VANET protocol 802.11p used and real time packet classification of DoS attack in VANET is identified by detection of jammer node using beacon exchanges (LYAMIN, N et al., 2014). The Wireless network to mitigate selective jamming attack packet hiding queue (DIVYA, S and Gosul, M, 2012) is adapted. The queue consists of list of wirelessly connected nodes of network. Nodes lying within Communication range are able to communicate directly or indirectly with hopping in the case of outside the range. Nodes use both unicast and broadcast modes for communication. Communication is secured by encryption if required or it is kept unencrypted. To provide (symmetric) encryption, keys are shared among communicating receivers. Also asymmetric pre shared key pairs are used to establish communication security.
2.3 Security in Wireless Network

Security of Wireless Network is a research issue due to its open nature. Wireless Network is vulnerable to attacks due to its characteristics. Jamming attack in WLAN can be performed under two models: External threat model and internal threat model. Various cryptographic primitives are used to develop anti jamming algorithm (GOLDREICH, O, 2004; NADEEM, Aamer, 2005). DES, AES, RSA and MD5 are used at different level in commitment methods, development of cryptographic puzzle method, all or nothing strong hiding method by cutting whole message in to small parts and applying padding and encryption function. In Real time packet classification at Physical layer and MAC Layer, MAC header portion is to be encrypted by using symmetric key algorithm between sender and receiver which is a public key algorithm. Asymmetric key algorithm is also used in which key pair is distributed by base station to sender and receiver. SHCS uses symmetric key and size of key is such a way that computational and communication overhead is to be kept low. Security of CPHS depends on the hardness and computational ability of solver. In this scheme security is independent of Physical layer characteristics. Time to Solve $t_p$ and $k$ key size is to be send with packet. Solver tries to reverse the process to extract the real message and compare computational time with $t_p$ and result $m_2$ with received message $m$. This scheme has high computational and communication overhead. AONT–HS use publicly known symmetric key in which message $m$ is cut down in different parts $m_1, m_2, \ldots, m_n$ and all parts are applied with encryption algorithm and at receiver side all parts are applied decryption and combined to make a final message $\tilde{m}$. AONT-HS has modest computational and overhead. Random key distribution methods are used as asymmetric key algorithms in which it hides location of control channel (JOSHNA, S et al., 2013)

We have performed comparison of different encryption algorithms. This helps for selection to implement in cryptographic primitives. Encryption Algorithms for security during communication plays important role. Text file
of different size in Table 2.1 is taken as an input and results are checked and computational time, memory usage (Overhead) and battery power is the criteria to compare. AES gives more security and less computation time compare to DES and RSA (GURPREET SINGH and Supriya, 2013) Comparative study of DES, 3DES and AES is done for nine different factors in Table 3.3 and based on it (O. ALANAZI et al., 2010), it shows that AES is better compare to DES and 3DES and with four factors in Table 3.2 key length, block size, speed and Security (GURPREET SINGH and Supriya, 2013) AES provides more security with lowest CPU power than other algorithms (N., Ferguson et al., 2001)

Table 2.1 Comparisons of AES, DES and RSA in terms of Time and Memory

<table>
<thead>
<tr>
<th>Data (kB)</th>
<th>DES (Sec.)</th>
<th>AES (Sec.)</th>
<th>RSA (Sec.)</th>
<th>DES (KB)</th>
<th>AES (KB)</th>
<th>RSA (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>1.81</td>
<td>2.02</td>
<td>9.45</td>
<td>84,261</td>
<td>80,912</td>
<td>90,814</td>
</tr>
<tr>
<td>64</td>
<td>1.83</td>
<td>2.13</td>
<td>10.53</td>
<td>66,531</td>
<td>61,544</td>
<td>76,117</td>
</tr>
<tr>
<td>128</td>
<td>2.03</td>
<td>2.29</td>
<td>11.41</td>
<td>54,395</td>
<td>52,902</td>
<td>55,178</td>
</tr>
<tr>
<td>256</td>
<td>2.14</td>
<td>2.47</td>
<td>16.27</td>
<td>22,189</td>
<td>15,679</td>
<td>25,891</td>
</tr>
<tr>
<td>512</td>
<td>2.43</td>
<td>2.63</td>
<td>24.44</td>
<td>41,113</td>
<td>33,207</td>
<td>43,321</td>
</tr>
</tbody>
</table>

Table 2.2 Comparisons of AES, DES, 3DES and RSA (based on features)

<table>
<thead>
<tr>
<th>Features</th>
<th>RSA Created By</th>
<th>DES Key Length</th>
<th>3DES Key Length</th>
<th>AES Key Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created By</td>
<td>Ron Rivest, Adi Shamir, and Leonard Adleman In 1978</td>
<td>Depends on number of bits in the modulus n where n=p*q</td>
<td>56 bits</td>
<td>168 bits (k1, k2 and k3) 112 bits (k1 and k2)</td>
</tr>
<tr>
<td>Key Length</td>
<td>IBM in 1975</td>
<td>IBM IN 1978</td>
<td>Vincent Rijmen, Joan Daemen in 2001</td>
<td></td>
</tr>
<tr>
<td>Round(s)</td>
<td>1</td>
<td>16</td>
<td>48</td>
<td>10 - 128 bit key, 12 - 192 bit key, 14 - 256 bit key</td>
</tr>
<tr>
<td>Block Size</td>
<td>Variable</td>
<td>64 bits</td>
<td>64 bits</td>
<td>128 bits</td>
</tr>
<tr>
<td>Cipher Type</td>
<td>Asymmetric Block Cipher</td>
<td>Symmetric Block Cipher</td>
<td>Symmetric Block Cipher</td>
<td>Symmetric Block Cipher</td>
</tr>
<tr>
<td>Speed</td>
<td>Slowest</td>
<td>Slow</td>
<td>Very Slow</td>
<td>Fast</td>
</tr>
<tr>
<td>Security</td>
<td>Least Secure</td>
<td>Not Secure Enough</td>
<td>Adequate Security</td>
<td>Excellent Security</td>
</tr>
</tbody>
</table>
Table 2.3 Comparisons of Symmetric Block Cipher Algorithms (AES, DES and 3DES)

<table>
<thead>
<tr>
<th>Factors</th>
<th>AES</th>
<th>3DES</th>
<th>DES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key length</strong></td>
<td>128, 192, 256 bits</td>
<td>168 bits (k1, k2 and k3) 112 bits (k1 and k2)</td>
<td>56 bits</td>
</tr>
<tr>
<td><strong>Cipher Type</strong></td>
<td>Symmetric Block Cipher</td>
<td>Symmetric Block Cipher</td>
<td>Symmetric Block Cipher</td>
</tr>
<tr>
<td><strong>Block Size</strong></td>
<td>128, 192, 256 bits</td>
<td>64 bits</td>
<td>64 bits</td>
</tr>
<tr>
<td><strong>Developed in year</strong></td>
<td>2000</td>
<td>1978</td>
<td>1977</td>
</tr>
<tr>
<td><strong>Cryptanalysis</strong></td>
<td>Strong against differential, truncated</td>
<td>Vulnerable to differential. Brute Force attacker could analyze plain text using differential cryptanalysis</td>
<td>Vulnerable to differential and linear cryptanalysis Weak substitution tables</td>
</tr>
<tr>
<td><strong>Resistance</strong></td>
<td>Considered secured</td>
<td>One only weak which is Exit in DES</td>
<td>Proved inadequate</td>
</tr>
<tr>
<td><strong>Possible Keys</strong></td>
<td>$2^{128}$, $2^{192}$ or $2^{256}$</td>
<td>$2^{112}$ or $2^{168}$</td>
<td>$2^{56}$</td>
</tr>
<tr>
<td><strong>Possible ASCII printable characters</strong></td>
<td>95^{16}, 95^{24} or 95^{32}</td>
<td>$95^{14}$ or $95^{28}$</td>
<td>$95^7$</td>
</tr>
<tr>
<td><strong>Time required to check all possible keys at 50 billion keys per second</strong></td>
<td>For a 128-bit key: 5 x $10^{17}$ years</td>
<td>For a 112-bit key: 800 days</td>
<td>For a 128-bit key: 400 days</td>
</tr>
</tbody>
</table>

As the comparative analysis concludes AES is better than DES, 3DES and RSA as asymmetric key encryption algorithm in many features.

### 2.4 Well-known Cryptographic Primitives

#### 2.4.1 SHCS

SHCS is a strong hiding commitment scheme (JOSHNA, S et al., 2013), which is designed using symmetric cryptography. The main inspiration is to serve the strong hiding property and at the same time decreasing computation and communication overhead.

Assume that sender $S$ has a packet $m$ for $R$. So initially $S$ constructs

$$(C, d) = \text{commit}(m),$$
Where \( C = F_k(\pi_1(m)) \), \( d = k \).

(2.1)

Here the \( F_k(C) \) (commitment function) is an off-the-shelf symmetric encryption algorithm, \( \pi_1 \) is a publicly known permutation and \( k \) is a randomly selected key of some desired key length \( s \).

The sender broadcasts cipher text \( \langle C \parallel d \rangle \), where \( \parallel \) denotes the concatenation operation. Upon reception of \( d \), receiver \( R \) computes

\[
m = \pi_1^{-1}(D_k(C))
\]

(2.2)

where \( \pi_1^{-1} \) is notation of the inverse permutation of \( \pi_1 \). To satisfy the strong hiding property, the packet carrying \( d \) is formatted so that all bits of \( d \) are modulated in the last few PHY-layer symbols of the packet. To recover \( d \), any receiver must have to receive and decode the last symbols of the transmitted packet, so preventing early disclosure of \( d \).

2.4.2 CPHS

Here cryptographic puzzles are used to create a packet-hiding scheme. Main aim of using the puzzle is to enhance security. When one is using this method then recipient of a puzzle has to perform a predefined set of computations before extracting information of interest. The time required for obtaining the solution of a puzzle depends on its hardness and the computational ability of the solver. Security provided by CPHS is independent of PHY-layer parameters which is main advantage of this method. However, it contains higher computation and communication overhead.

Let a sender \( S \) has to send a packet \( m \) for transmission. The sender selects a random key \( k \) of desired length. Sender \( S \) generates a distinct puzzle \( p = \text{puzzle}(k, t_p) \), where \( \text{puzzle}(\cdot) \) denotes the puzzle generator function which generates a new puzzle, and \( t_p \) is the time required to solve the generated puzzle. Parameter \( t_p \) is measured in units of time, and it’s directly dependent on the computational capability of the adverse node, denoted by \( N \).
and it is measured in computation operations per second. After creating the puzzle \( \mathbf{P}, (C, P) \) is broadcast by the sender (where \( C = E_k(m_1) \)). On the receiver side, any receiver \( R \) receives puzzle \( P_1 \) and solves the puzzle \( P_1 \) to get key \( k_1 \) and then calculate \( m_1 = \pi_1^{-1}(D_k(C)) \). If the decrypted packet \( m_1 \) is significant (i.e., is in the proper format, has a valid CRC code, and is within the context of the receiver’s communication), the receiver acquire that \( m_1 = m \). Else, the receiver discards \( m_1 \). Figure 2.1 show the details of CPHS.

![Diagram](image)

**Figure 2.1 Cryptographic puzzles-based hiding scheme (use case)**

### 2.4.3 AONT-HS

Here a solution based on All-Or-Nothing Transformations presents the least communication and computation overhead. Such changes were initially proposed by Rivets to back off brute force attacks against block encryption algorithms. An AONT serves as an openly known and totally invertible pre-processing venture to a plaintext before it is passed to an ordinary block encryption algorithm calculation.

A transformation \( f \), is mapping message \( m = (m_1, m_2, \ldots, m_x) \) to a sequence of pseudo messages \( m_2 = (m_1, m_2, \ldots, m_x) \), is an AONT if

- \( f \) is a bijection\(^1\),

- it is computationally infeasible to obtain any part of the original plaintext, if one of the pseudo messages is unknown, and

---

\(^1\) A bijection from the set \( X \) to the set \( Y \) has an inverse function from \( Y \) to \( X \). If \( X \) and \( Y \) are finite sets, then the existence of a bijection means they have the same number of elements.
- $f$ and its inverse is efficiently computable.

Packets are pre-processed by an AONT before transmission yet remains without encryption. The jammer can't perform the real time classification until all pseudo messages related to the original packet has been delivered and the Inverse transformation has been performed. Fig 2.2 shows the details of AONT-HS.

![Figure 2.2 AONT-based hiding scheme](image)

2.4.4 Random Key Distribution

We propose the utilization of arbitrary key distribution to conceal the location of control channels in time and/or frequency. Here assessment of execution measurements of flexibility to control channel jamming, recognition of compromised clients, and deferral (delay) because of jamming as a function of the compromised clients.

2.4.5 Hidden Layer between Physical and MAC layer

In WLAN protocol 802.11 complete packet (see appendix) is received at MAC layer. So during real time packet classification at physical layer by showing few bits, it is easy to collect information of sender and receiver and jam the network.
So by using different level of permutation and encryption algorithm hidden sub layer is added between Physical and MAC layer to enhance security.

2.5 Research challenges

With the emergence of global connectivity and growth of usage of multimedia and real time application, Good QoS from Computer network is a challenging task. Wireless network is providing any time anywhere connectivity. Open nature of wireless network is more prone to the attacks and jamming in the network. Selective Jamming Attack from the adversary node is an internal threat to the network and cause for network performance degradation. Security in wireless network and network throughput is a big concern to both users and network designers. Major research challenges to design of Anti jamming algorithm include Jammer detection, Jammer localization and anti-jamming measures. The Proposed algorithm for prevention of selective jamming attack in wireless network is to be developed to improve QoS parameters for wireless LAN for achieving: better security in network, optimize network design and improve network performance for getting better QoS on various traffic of network. Various challenges occur during development of the proposed anti-jamming algorithm.

- *Detection of jammer in wireless network*
Selective Jamming attack is a part of internal threat model in which jammer is acting as an adversary node. Adversary node is a part of the wireless network. It is active as a regular node for some time and it is active as a jammer for some time in random manner. The detection of the jammer node in wireless network is a challenge.

- **Security threats in wireless network**
  Selective Jamming attack is done by adversary node in the wireless network. It is a part of internal threat model in which jammer is acting as an adversary node. It is active as a node for some time and also it is active as a jammer in random manner. Adversary node has an internal knowledge of the network and able to capture important messages of Route Request / Route Reply messages or TCP acknowledgement of TCP sessions.

- **Real time classification of packets at Physical layer**
  Adversary node has an internal knowledge of the network and able to capture important messages of Route Request/Route Reply messages or TCP acknowledgement of TCP sessions. Packets are identified by first few bits at physical layer by jammer and cause for Denial of Service (DoS) in the network.

- **Performance optimization issue in wireless network**
  Selective Jamming attack in wireless network effects network performance. Due to jamming, various QoS parameters related to network performance degrades.

- **Finding the alternate path based on routing protocol**
  Wireless network supports various routing protocols AODV, DSDV and DSR at routing layer to route the packets.
2.6 Analysis and Findings

External threat model is the one in which jammer node performs the jamming activity from outside the target network. So it is easy to attack on wireless network also decreases the probability of being identified as an attacker.

Spread-spectrum techniques such as frequency hopping spread spectrum (FHSS), or direct sequence spread spectrum (DSSS) can be used PHY layer for protection of wireless transmissions from jamming. SS provides security against interrupt to some extent (typically 20 to 30 dB gain), still an efficient jammer is capable of jamming data packets of one’s selection.

Communication in wireless network is done by broadcasting the message. In internal threat model, jammer is a part of network and does passive attack. It has knowledge about network and acts randomly. Some times at as a proper node and sometimes as a jammer.

All the current anti-jamming methods are enhancing security in wireless network. Major current anti jamming algorithms do not improve performance of network. All the packet hiding methods SHCS, CPHS, AONT-HS and Random Key Generation use to provide some type of security at physical layer. The weakness of all the methods are more computational and Communication overhead. SHCS uses symmetric key and size of key is such a way that computational and communication overhead is to be kept low compare to all three method. Cryptographic Puzzle based hiding scheme (CPHS) depends on the hardness and computational ability of resolver. In this scheme security is not depends on Physical layer characteristics. Time to Solve $t_p$ and $k$ key size is to be send with packet. Solver tries to reverse the process to extract the real message and compare computational time with $t_p$ and result $m_1$ with received message $m$. This scheme has high computational and communication overhead.
AONT based hiding scheme (AONT–HS) use publicly known symmetric key in which message $m$ is cut down in different parts $m_1, m_2, \ldots, m_n$ and all parts are applied with encryption algorithm and at receiver side all parts are applied decryption and combined to make a final message $m$. AONT-HS has modest computational and overhead. Random key distribution methods are used as asymmetric key algorithms in which it hides location of control channel of wireless network.

AES is better than DES, 3DES and RSA as per comparison shown in Table 2.1, Table 2.2 and Table 2.3.

First level of Encryption method use symmetric key method AES in the proposed anti-jamming algorithm. Second level of Encryption method use asymmetric key method RSA for the key distribution in WLAN.