Smart Jamming-Negotiation of Specific Signal from Jammer.

[1]Vinoth Kumar V
vijayvinoth97@gmail.com
Assistant Professor

[2]Divya K
divyavarshan15@gmail.com

[3] Divya R
divyaravi1426@gmail.com

[4] Haripriya S
haripriyaselvam111@gmail.com

[2][3][4]UG students
Department of Computer Science and Engineering
T.J.S. Engineering College

Abstract

Secure neighbor discovery is a basic process in MANET deployed in an aggressive environment. Neighboring nodes can able to discover and authenticate each other in a secured manner. Anti-Jamming communication is possible but unknown to jammer. Initially transmit radio signals to prevent neighboring nodes from exchanging messages. JR-SND [Jamming Resilient Secure Neighbor Discovery] scheme is used. It is based on direct sequence spread spectrum and random spread code pre-distribution. To efficiently share the messages with secured processing. HDSR algorithm is used for minimizing the total energy required for end-to-end packet traversal and to increase the operational lifetime of the network.

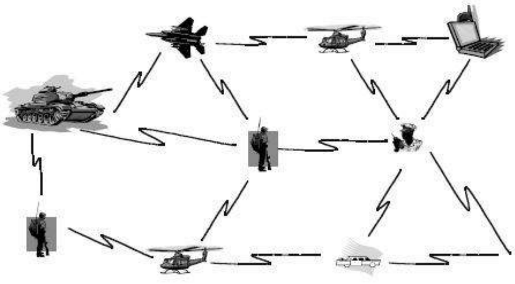
Index Terms – *Jamming, Secure neighbor discovery, MANET.*

1. Introduction

As the basis of other network functionalities such as medium access control and routing, secure neighbor discovery need to be frequently performed due to node mobility. We using open wireless medium in MANETs renders secure neighbor discovery particularly vulnerable to the jamming attack. Some solutions are designed in a centralized manner. The circular dependency between anti-jamming communication and spread code establishment are possible. Unique features of MANET neighbor discovery make these elegant solutions sometimes unsuitable. The adversary can use such public knowledge to inject neighbor discovery request in the whole network, leading to a special Denial of Service (DoS) attack in which all nodes are used to perform endless verifications of neighbor discovery request.

The observation is most MANETs are inherently different from the civilian application. Specifically, MANETs in hostile environment such as battlefields

are normally controlled by the same authority. During the network operation two neighboring nodes can use their spread codes to conduct anti-jamming secure neighbor discovery via DSSS communication.



Overview of Mobile Ad-hoc Network

2. NETWORK MODEL:

Due to node mobility, every node need periodically perform neighbor discovery to discover others within its transmission range. This implies that an incoming message spread using the code under real time monitoring can be de-spread with negligible delay. To prevent the adversary from impersonating legitimate nodes, neighbor discovery must be conducted in a secure fashion such that two nodes accept each other as mutual neighbors after authenticating each other's credentials issued by the MANET authority. There are many mutual authentication methods that suffice our purpose and often involve a three way handshake between two involved nodes.

ADVERSARY MODEL:

We assume an omnipresent adversary or jammer J aiming to jam neighbor discovery and thus prevent neighboring nodes from discovering each other anywhere in the network. J is assumed to be computationally bounded, which means that if J does not know the spread code being used. It is infeasible to recover exhaustive search within the network. J need transmit using the same code and also synchronize with the target transmission. In other words, J only needs to determine which spread code to use to jam transmission. Random jamming places no additional requirements on J's computation capability while receiving jamming requires J to identify the correct spread code being used before the end of the targeted message transmission. Besides jamming attack, the adversary may also exploit the operations of JR-SND to launch the DoS attack by injecting arbitrary fake neighbors-discovery requests to occupy legitimate nodes with endless verifications of these fake requests.

JR-SND DESIGN:

Spread Code Pre-Distribution:

Our scheme permits new nodes to join the network. In particular, the authority can assign the spread codes of a virtual node to a unique new node. If there are more than l' new nodes, the authority can conduct the previous distribution process for each additional w new nodes with existing s codes, which will result in every code being shared by one more node.

D-NDP: Direct Neighbor Discovery Protocol:

During the network operation, each node periodically initiates neighbor discovery in a randomized manner. Assume that A initiates the D-NDP process prior to B. Starting from a random time point; A repeatedly broadcasts a HELLO message for r rounds, where r is a system parameter.

M-NDP: Multi-Hop Neighbor Discovery Protocol:

Two physical neighbors may fail to directly discover each other via D-NDO either because they have no common spread codes or because J has compromised their common spread codes whereby to successfully jam the D-NDP message transmission. Jamming-resilient path connecting along with every two adjacent nodes have discovered each other.

3. Literature Review

Basically in all the directions radio frequency electromagnetic wave communication has been resistance to prevent before an attack. In jamming use of secret key shared by sender and receiver. There is no method for achieving jam resistance without the shared key. In this wireless communication able to reach higher level such as secret key are becoming impractical. The civilian side of the global positioning system cannot use a shared secret key. So that military secret is GPS cannot be protected from jamming. They used FAA (Federal Aviation Administration) is responsible for advancement and regular of civil aviation as well as overseeing development of air traffic control. The information rate can be transmitted over a given bandwidth in a specific communication. Designed to prevent being jammed based on code controlled frequency. Unlike conventional frequency hopping system where hopping patterns are determined by preselected pseudo-random sequences. It retrieves the pattern without prior knowledge through decoding and encoding process. Due to the combination of dynamic frequency hopping and coding system can effectively mitigate random jamming inference. It maintains high spectral efficiency.

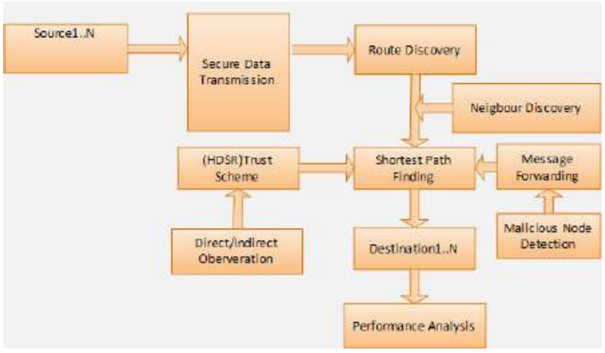
4. Existing System

The existing system is based on some publicly known communication strategies such as public spread code sets. The adversary can use public knowledge to inject arbitrary many neighbor requests in the whole network, leading to a DoS attack in which all nodes are forced to perform endless verifications of neighbor discovery requests. Existing approaches are not scalable. They do not cover group communication. To transfer the message efficiently in a secured manner preventing from denial of service attack. Throughput and packet delivery ratio can be improved significantly with slightly reduced average end to end delay and routing overhead of messages. It can reliable and also block coding is applicable.

5. Proposed System

We propose recent advances in trust management schemesthat enables the security in MANET. In trust management scheme we use HDSR[Hybrid Dynamic Secure Routing Protocol]. It has two components:Trust value in direct observation,trust value in indirect observation. In direct observation the trust value is derived using bayesian inference.Indirect observation is derived using Dempster shafter theory. Combining these two components we can getaccurate trust value.Simulation result show that throughput and packet delivery ratio will be improved and to reduce end to end delay and overhead of messages.

Fig 5: System Architecture



Source node sending through secured data transmission and it discovers the route. The neighbor discovery node has been discover and finding the shortest path routing. In this HDSR trust scheme have been included then the malicious node are detected and it forwards the message. Finally the message transferred to destination and performance is being analyzed. There are two types of observation in trust management scheme which is direct observation and indirect observation.

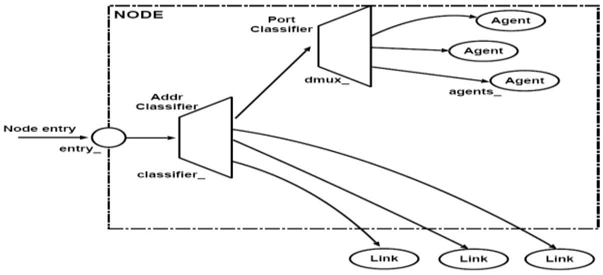


Fig 5.1: NS2 internal schematic diagram

This recursive function can be used to decode all the messages found in a given packet by calling BBC Decode (1). There must be a global M (1…m+k) which is a string of m+k bits. The number of bits in a message is m, and the number of checksum zeros appended to the messages k. H is a hash function. The definition of H and values of m and k are public not secret. The definition of indelible mark and location are specific to the physical instantiation of BBC used. An attacker can also broadcast such pulses but cannot erase any existing pulses. Such pulses are difficult to erase because they are short, very high power, and consists of unpredictable random noise with energy spread over the entire spectrum no known system exists that can detect and analyze such pulses and then send out an inverse way form to cancel them.

Algorithm 1: BBCdecode (n)

```
if n=m+k+1 then
else
if n>m then
limit←0
else
limit←1
end if
for i←0…limit do
   M[n]←i
   If there is an indelible mark at location
   H (M [1…n]) then
      BBCdecode (M, n+1)
end if
end for
end if
```

5.2. Neighboring node on network performance:

The process of identifying the nodes located in the communication range of a given node. Consequently the correctness of neighbor discovery has a major influence on the network performance. It is vulnerable to security threats. The local topology affected by wormhole attack cannot embed to the space with a good fit.

Algorithm 2: Detect Ranges Larger than R

```
t ←Current time
D ← Diss (t) from Algorithm 1
procedure DETECT RANGES LARGER THAN R
    DirectWormholeFlag ←False
    [DirectIndirectList] ← [ ]
    for I = 1→N do
        if D (N+1)I > R then
            DirectWormholeFlag ← True
            [DirectIncorrectList] ← i
        end if
    end for
end procedure
```

5.3. Wormhole Attack:

Wormhole attack are very powerful because the attacker does not need to compromise any legitimate needs to launch the attack and also encrypting messages would not help to prevent the attack since the attacker does not needs to determine the content of messages. We design suitable geometry test to locate the inconsistencies caused inherently by the attack to the ranging information to detect the attack and localize the links. Actually the pair wise distance measured by two nodes will be sum of distances which each node perform wormhole end plus a small random value relevant to the delay of transmission between the two wormhole ends. The network consists of a number of mobile nodes initially distributed randomly in the network field. After the network deployment, nodes move based on mobility that it can directly communicate with and verifies the correctness of its neighbors using our mechanisms. Our protocol is independent and distance measures are performed. Each node also needs a clock having precision of hundreds of microseconds for the timing purposes required by the ranging operation. The RF and US Interfaces of the nodes have transmission and reception ranges of R. The idea can be applied to a topology in any dimensions. It is not possible for the attacker to escape from being deducted by the protocol by manipulating the ranging values. Some solutions are designed in a distributed manner. It has lower complexity when compared to lower works in a secured manner.

Algorithm 3: Gathering Ranging Information by node A

```
t←Current time
procedure RANGING
    (dist)←measure distance to each neighbor
    N←No of neighbors
    Broadcast (dist)
    Save (dist) matrices received from neighbors
end procedure
procedure CREATE DISIMILARITY MATRIX (Diss)
    for i=1-->N do
        for j=1→N do
            (Dij)←distance between ith and jth neighbors
        end for
    end for
    Diss (t)←D
    Neighbors (1:N)← I D s of neighbors
    Neighbors (N+1)← Node A
    I DList (t)←neighbors
end procedure
```

In a direct sequence a sender uses all frequencies simultaneously by combining the message with a pseudorandom bit stream, generated according to some key. This is used in CDMA (Code Division Multiple Access). The message is encoded in the exact timing of the pulses dependent upon a secret key if jam resistance is desired. The scaling problem is even worse for military applications.

5.4. Performance under fading nodes:

If the node is used to run the protocol for the first time in the network life, it would list the coordination of the whole points in the MDS output as points to fit the plane. If the length of the list is larger than the specified parameter. Since the protocol identifies the inconsistent ranging values, to evade the wormhole detection mechanism the adversary has to avoid making inconsistencies to the ranging information when relaying ranging messages. Our algorithm works in a distributed manner such that a node can use local ranging information of its neighbor nodes to verify all its neighbors in a single run. The computational complexity of our protocol is lower than the complexity of the relevant state of art solutions. Some solutions are designed in a centralized manner. The connectivity information gathered all the nodes is sent to a single point and gets processed centrally to detect the wormhole attack. The number of links added to the network lets this mechanism to detect and locate the attack. Each node can verify its one neighbors having its local neighborhood information.

Algorithm 4 :Detection in neighborhood of node

```
Run
Incorrect List (t) ←[ ]
Correct List (t) ← [ ]
procedure PERFORM 3D MDS
 Topology (1: N+1) ← MDS (D,P=→3)
 IF time==0 then
 Points Fits Plane ← Topology (1: N+1)
else
 PointsFitsplane ←T  Correct List (t-1)
if size (PointsFitsPlane) <Np then
Add Np size (PointsFitsPlane) random points
end if
end if
for i=1 →N do
if l (i) > then
Incorrect List (t)← i
else
CorrectList (t)← i
end if
end for
else if DirectWormholeFLAG = = True then
for i=1→ N do
IncorrectList (t)→ i
else
Correct List (t)→ i
end if
end for
else
for i=1→N do
Correct List (t)← i
end for
end procedure
```

6. Conclusion

Finally, it proposes resent advances in trust management scheme that enhances the security in MANET. In the trust management scheme we use hybrid dynamic secure routing protocol (HDSR) it has two components: Trust value in direct observation and trust value in indirect observation. In direct observation the trust value is derived using Bayesian inference and indirect observation the trust value is derived using dempster-shafer theory. Indirect observation is also called as second hand information.

9. References

[1] H. Wang, L. Zhang, T. Li, and J. Tugnait, "Spectrally efficient jamming mitigation based on code-controlled frequency hopping," *IEEE Trans.Wireless Commun., vol. 10, no. 3, pp. 728–732, Mar. 2011*

[2] R. Pickholtz, D. Schilling, and L. Milstein, "Theory of spread-spectrum communications-A tutorial," *IEEE Trans. Commun., vol. COM-30, no. 5,*pp. 855–884, May 1982.

[3] P. Papadimitratos *et al., "Secure neighborhood discovery: A fundamental* element for mobile ad hoc networking," *IEEE Commun. Mag., vol. 46,* no. 2, pp. 132–139, Feb. 2008.

[4] L. Xiao, H. Dai, and P. Ning, "Jamming-resistant collaborative broadcast using uncoordinated frequency hopping," *IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 297–309, Feb. 2012.*

[5] Leemon C.Baird III, William L.Bahn, Michael D. Collins, Martin C. Carlisle, Sean C. Butler "Keyless Jam Resistance"NY 20-22 June 2007.