# Cross Layer Security with Stable Path Selection (CSSPS) Mechanism in UWB MANET

**Sunita Usturge-Nandgave, T. Pavankumar**

***ABSTRACT---MANET doesn't need any framework, it's miles multi-jump system of cell hubs. every hub can stream openly at any heading. we are equipped for utilize remote contraptions which comprise of versatile, PDA, tablet, pc and so forth wherever whenever. MANET with portability trademark has severa challenges, which include dynamic topology, data transfer capacity imperatives and limited battery power, etc. very tremendous Band MANET has applications in assortment of fields alongside unreasonable transmission capacity remote network for houses and workplaces. UWB can be connected in recreation and crisis administrations, military interchanges. UWB MANET hubs are dynamic and each hub demonstrations like a switch, due to changing over topology UWB MANET is helpless to noxious assault. Directing ambush will end up one of the exceptional problem in UWB MANET various steering convention SADOV calm AODV, SAOMDV loose AOMDV are throughout everyday life. some of these conventions have boundaries you may verify course anyway not verbal trade data. Proposed procedure will give both steering and correspondence security. This work of art manages a top to bottom assessment of system as far as parcel misfortune proportion, throughput and diminished steering overhead choice to directing assaults.***

***Keywords—UWB MANET, routing attack, AODV (Ad-hoc On Demand Distance Vector), grayzone, SNF, NCR, RSS..***

## I. INTRODUCTION

Ultra Wide Band (UWB) is a radio innovation to be applied in close to home region arrange maximum as of past due framework depending on extremely wide band innovation have became a promising hopeful in usage of MANET. this is for the most element because of their floor-breaking skills, for example, their excessive records quotes and occasional power utilization [4]. UWB devours [5] low energy levels and may be applied in short range, high facts switch ability (>500MHz). UWB [14] offers lengthy radio variety which is around 150 meters indoor and 1 KM outdoor and high records price extra than one hundred Mbps with bit fees of 55, one hundred ten and 2 hundred Mbps [5]. UWB utilized in slicing aspect Bluetooth innovation devices. it works on low energy devices. UWB hub positions region themselves no need of GPS. it is moreover appropriate for indoor and outside application [14]. UWB highlights: suitable statistics switch ability usage, and maximum excessive transmission variety is 250m [14], least transmission variety is 10m and recurrence variety is three.12GHz to 10.6GHz. A flimsy connection [8] and safety of connection are the precept issues of UWB. MANET has problems in channel project and utilization, nonattendance of foundation, hubs are often shifting and topology is evolving continuously. each hub in a MANET is match for going about as a transfer [2]. one of the angles, for example, directing having one-of-a-kind security concerns hub helplessness (assault) is workable.

steerage in MANET: every hub fills in as a transfer in MANET. Directing overhead receives reduced contrasted with stressed structures. Sender and collector hubs can communicate with each other if and simply within the event that they're inside the correspondence scope of one another; at the off chance that they're not, the sender needs to ship the message via center of the street hubs. Capricious and dynamic nature of MANET, [12] hubs don't have any in advance data approximately topology; in this way, hubs need to decide the topology. A hub [7] announces its essence and tunes in to classified ads of its buddies. that is the way by means of which a hub finds its friends just as strategies to come back to those. steerage is a chief check in the state of affairs wherein hubs are shifting generally. Proactive directing, as an instance, DSDV and OLSR [8] now and again sends steerage manipulate parcels to associates for fresh steering tables. these are table driven.

Receptive steering conventions, for instance, AODV and DSR ship manage parcels just whilst direction revelation or course help is completed. these are on hobby.

Because of absence of confided in focused corporation, constrained transfer speed, confined strength, far flung connections, dynamic topology, and simple listening stealthily MANET hubs are more helpless to safety attacks than existing ordinary structures.

A hub may have a valid path in grayzone region however join among the hub and it's next bounce is shaky. package deal misfortune share is additionally excessive right here. Hazy area territory happens while a hub try and move beyond its transmission run. Gotten signal best is applied as go layer metric to expect interface dependability. move layer technique is applied to present low layer records to actualize directing technique with the aid of recognizing and foreseeing the occasion of correspondence dim zones. In such vicinity Packet Loss Ratio (PLR) is excessive. on the factor while a route bombs course revelation is restarted in AODV at that point bundles wander off. this is one of the clog causes. on this manner a need is raised to control parcel misfortune.

on this paper pass layer security with solid manner desire instrument is broke down. The paper is sorted out as below: place 2 speaks to specific directing attacks in UWB

**Revised Manuscript Received on June 10, 2019.**

**SunitaUsturge-Nandgave,**Research Scholar, CSE Department, K L University, Guntur, Andhra Pradesh, India. (snandgave@gmail.com)

**Dr. T. Pavankumar,** Professor CSE Department, K L University, Guntur, Andhra Pradesh, India.(pavankumar_ist@kluniversity.in)

MANET, at the same time as phase three demonstrates usage move layer security of direction making use of solid manner choice instrument solid Neighbor Frequency(SNF), Neighbor alternate Ratio (NCR), received signal strength (RSS). segment four speaks to pastime condition with parameters. moreover speaks to end result exam. section five finally ends up this paper.

## II. ROUTING ATTACK IN UWB MANET

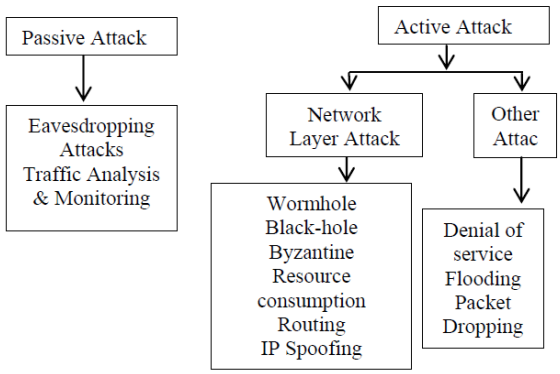


**Figure 1: Routing attacks in UWB MANET**

Routing Attacks mainly classified as passive and active attack.

**Passive attacks** obtains information without disturbing normal network operation and difficult to detect.

**Example:** Traffic analysis, traffic monitoring, and eavesdropping

Traffic analysis attacker tries to sense the communication path between the sender and receiver [13].

Traffic monitoring attacker can read confidential data but cannot edit.

MANET eavesdropping finds out the secret data such as private or public key of sender, receiver or any secret data.

**Active Attacks** can disturb network operation by modifying or deleting information, injecting a false message or impersonating a node.

**Example:** Modification, impersonation, fabrication, jamming and message replay.

Fabrication attacks a malicious node generates false or incorrect information. Jamming attack occurs at physical layer.

Message replay malicious node repeat data or delayed data even intercept password as well.

This paper mainly focuses on routing attacks.

*A. Routing attacks:*

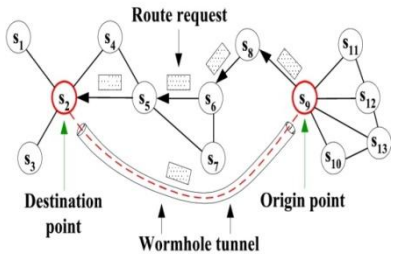


**Figure 2: Wormhole Attack**

In wormhole attack malicious node connect two disjoint points in space, here also in the same way in MANET one or more attacking nodes disrupt routing by short-circuiting the network.

*Solution to wormhole attack:*

*i) Geographical leashes & temporal leashes*

A leash is added to each packet to restrict distance the packet allowed to travel. A leash is associated with each hop. Each transmission of a packet requires the new leash. A geographical leash limit the distance between transmitter and receiver of packet. A temporal leash provides an upper bound on a lifetime of a packet.

*ii) Using directional antenna*

Restrict direction of signal propagation through air to avoid packet dispersion.

*A. Blackhole attack:*

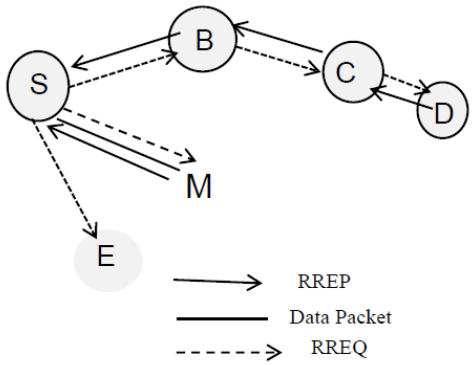


**Figure 3: Black-hole Attack**

In black-hole attack malicious nodes acts like a black-hole which drops all data packets passing through.

**Solution to black-hole attack:**

Maintain a table in [15] each node with previous sequence number in increasing order. Each node before forwarding packet increase sequences number. The sender node broadcast RREQ to its neighbor and once RREQ reaches it replies with RREP with last packet sequence number, if the intermediate node finds that RREP contains a wrong sequence number it understands that somewhere something went wrong.

*B. Byzantine attack:*

A set of intermediate node work between a sender and receiver performs some changes such as creating routing loops, sending packets through non-optimal path for selectively dropping packet which disrupt routing services.

*C. Spoofing*

Malicious nodemis-present his identity so that sender change the topology.

*D. Sybil attack:*

In Sybil attack malicious node manifest itself by faking multiple identities by pretending to consisting of multiple nodes in the network. One single node can assume a role of multiple nodes and can monitor or hamper multiple nodes at a time.

*Solution to Sybil attack:*

Maintaining chain of trust so single identity is generated by a hierarchical structure.

*E. DOS attack:*

Denial of Service (DOS) attack, malicious node consumes bandwidth of the network. When a message from unauthenticated node comes, then receiver will not receive that message because he is busy and beginner has to wait for the receiver's response.

*F. Flooding attack:*

The attacker node floods the network with a high quality route with a powerful transmitter.

*G. Jellyfish attack:*

Attacker node reorders some of the packets before forwarding them.

*Solution to Jellyfish attack:*

2ACK, where S sends data packet to D, Destination will send back a special two hops acknowledge indicating data received.

## III. THE PROPOSED METHODOLOGIES

The aim of proposed algorithm is to detect rushing attack and to improve performance of the network in terms of Packet Loss Ratio, throughput, Packet Delivery Ratio and Normalized Routing Load.

*PSEUDO CODE*

Step 1: Initialize source and destination number of node list, threshold of link length.

Step 2: broadcast RREQ in network

Step3: Compute node authentication using digital signature

Step 4: all nodes in communication computes message digest (MD) using MD5 algorithm.

Step 5: select authenticated node having high SNF and NCR in network.

Step 6: Find all path and analyze the path. If path is not candidate path i.e. final path (shortest path) then choose a path randomlyfrom available path list.

Step 7: If SNF of path >SNF_threshold

Step 8: insert path in candidate_path_ list and check Source node MD = Destination Node MD

Step 9: end if

Step 10: end for

Step 11: if candidate_path_list != NULL then

Step 12: Choose shortest path as randomly

Step 13: if both Messages digest match then communicated data is correct.

Step 14: stop.

The proposed protocol (CSSPS) depends on SAODV and SAOMDV to accomplish the steady way. In unique SAODV course disclosure process when connection is broken whether nearby reclamation or re-course revelation of source hub, all will prompt transmit a ton of course solicitation messages in system. Consequently control overhead is there. To lessen control overhead, we have included Neighbor Change Proportion (NCR) is embedded into hi messages. Source hub sends Hi messages are utilized to distinguish the neighbors. Hubs having most elevated NCR worth are refreshed into neighbor table. In the wake of refreshing the neighbors source communicates steering solicitation to high NCR neighbor hub. This neighbor will check got signal quality of steering solicitation is more noteworthy than limit at that point begin bounce tally discovery generally dispose of the bundle. In jump tally recognition bounce tally is checked by (rq_hop_count – rt_advertised_hops) is more noteworthy than resistance jump tally. If not go for circle free recognition or else dispose of the RREQ parcel. Following stage is turn around course table is refreshed with the RREQ message. Connection solidness factor (LSF) is embedded into reverse_LSF_list, likewise stable neighbor recurrence (SNF) is additionally checked. SNF is tally how often the specific hub is comes in course disclosure process. Next check is on whether current hub is goal or not. In the event that it is goal, at that point produce RREP with LSF. Generally same procedure of broadcasting proceeded, till goal or middle of the road hub with crisp course to goal is acquired. When course to goal is discovered at that point course dependability factor RSF is determined. Same procedure rehashed for different courses and their individual RSF's are determined. Toward the finish of the course revelation procedure course with biggest RSF worth will be picked as definite course to the goal. Presently source can send information along this way to goal.

In the proposed framework, in the wake of making course from source to goal another worry is security of both directing and conveying hubs. The system is intended to permit existing system and directing conventions to play out their capacities, while giving hub verification utilizing advanced mark, get to control unauthenticated hub kept out of system, and correspondence security can be accomplished utilizing HMAC Hash based Message Validation Code instruments.

## IV. RESULTS &DISCUSSIONS

### A. Simulation Condition

Reproduction is led utilizing NS-2.29 (802.15.4) for UWB MANET. Four conventions are mimicked and thought about the outcome. These conventions are SAODV, SAOMDV, SRSSP and proposed convention.

The exhibitions of CSSPS, SRSSP, SAOMDV and SAODV are contrasted with deference with three measurements: parcel misfortune proportion, normal start to finish delay, throughput, Standardized steering burden and Bundle conveyance proportion.

The PLR is characterized as a proportion of the quantity of lost bundles to the all out number of transmitted parcels.

Normal start to finish delay: This is the normal time delay for information parcels from the source hub to the goal hub.

Normal throughput: It is the normal number of messages effectively conveyed per unit time number of bits conveyed every second.

Standardized steering load: The standardized directing

burden is characterized as the portion of all steering control parcels sent by all hubs over the quantity of got information bundles at the goal hubs. This measurement reveals how effective the directing convention is. The bigger this division is, the less effective the convention is.

Parcel conveyance proportion: This is the quantity of bundles sent from the source to the quantity of got at the goal.

The reenactment results includes arrange topology with shifting number of hubs 25, 50, 75, 100, 125. There are diverse source hubs speaks with the goal hub. Versatility situations can be produced by arbitrary waypoint model in reproduction territory 1000m *1000m.The recreation parameters are as appeared table 1.

**Table 1. Simulation Parameters**

| Parameter | Value |
|---|---|
| Simulation Time | 200 s |
| MAC Layer | IEEE 802.15.4 |
| Channel Bandwidth | 1Mbps |
| Transmission range | 250m |
| Simulation area | 1000x1000m |
| Number of static node | 2 |
| Number of mobile node | 25, 50, 75, 100, 125 |
| Pause time | 1s |
| Maximum speed | 1m/s |
| Application | CBR |
| Packet Size | 512 bytes |
| Number of CBR flows | 3, 5, 10, 15, 20 |
| allow-hello | 3 |
| hello-interval | 3 s |

*A. Simulation Results*

The random topology is shown in Figure 3 in which 70 nodes are placed in an area of 1000 m *1000 m. nodes move according to the random waypoint mobility model with max speed 1 m/s. We make the source –destination pairs by increasing from 3 to 20 (i.e.) 3, 5, 10, 15 Tolerance_ Hop is set to 2.

*PLR for random topology:*

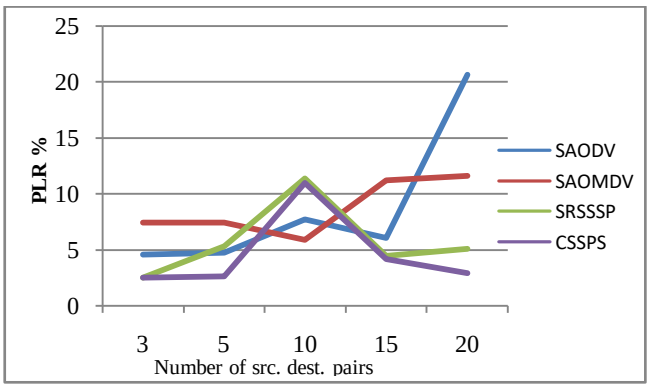


**Figure 4: PLR for random Topology**

Figure 4 demonstrates that CSSPS, SRSSSP achieves much better PLR performance than SAODV and SAOMDV and outperforms it from 19.59% to 54.33

*End to end delay for random topology:*

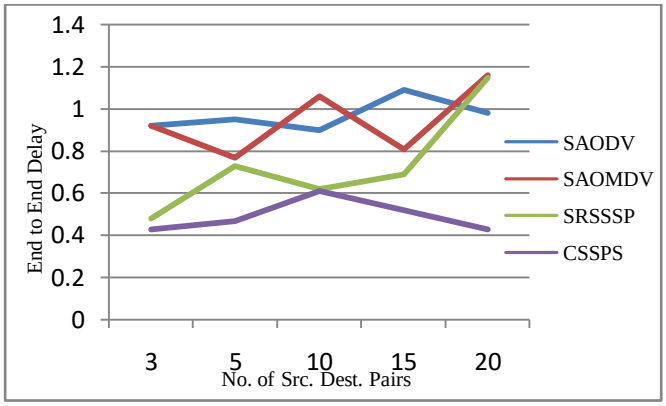


**Figure 5:End to End Delay for random topology**

The average cease-to-stop cast off of CSSPS, is typically lower than SRSSSP, SAODV and SAOMDV that is proven by using determine four The motive comes from additives (1) CSSPS is capable of select out extra dependable direction than SRSSSP, SAODV and SAOMDV at some point of path discovery process and (2) in SAODV and SAOMDV, route rediscovery is initiated simplest after the cutting-edge course has detected to be damaged.

Such method is pricey (the manage overhead and the retransmission/ timeout time). Preemptive course protection can reduce the latency of detecting a broken route if the alternative course is decided earlier than the real path breaks. In CSSPS, opportunity route discovery is completed collectively with location machine and NCR which gives a excessive performance of time usage. the short community direction repair gadget need to pick out a reliable alternative direction amongst candidate paths to create or replace the direction desk access of corresponding nodes.

*Normalized routing load for random topology:*

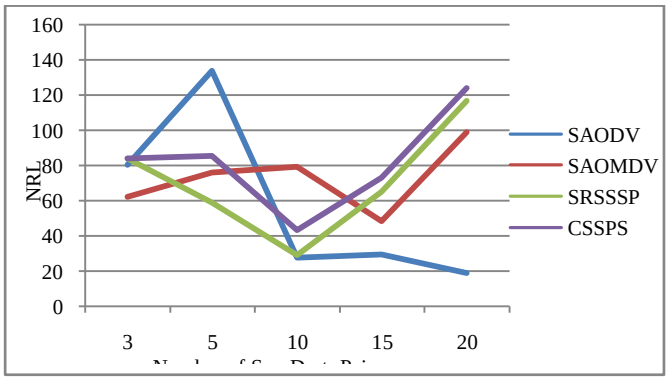


**Figure 6 Normalized Routing Load for random topology**

Figure 6 shows the normalized routing load. SAODV has a higher normalized routing load than SRSSSP and CSSPS in the case of5 to 15 source-destination pairs.

*Throughput for random topology:*

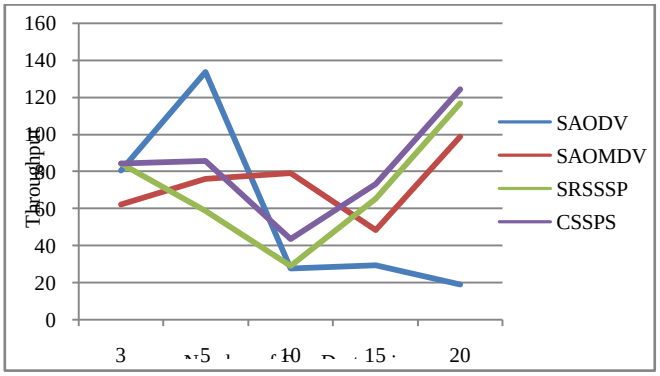


**Figure 7 Throughput of random topology**

Figure 7 illustrates the throughput performance ofSRSSSP, SAODV and SAOMDV. The throughput of CSSPS does not suffer from degradation and performs more stable compared with that of SRSSSP, SAODV and SAOMDV.

*Packet delivery ratio for random topology:*

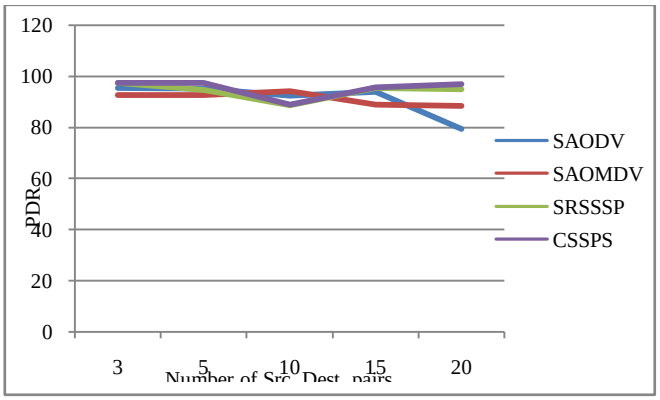


**Figure 8 PDR of Random Topology**

As shown in figure 8 Packet Delivery Ratio of CSSPS is better than RSSSP, SAODV and SAOMDV. Here SAODV and SAOMDV shows least PDR for large source-destination pairs, performance of SAODV and SAOMDV is better but as comparing to SRSSSP and CSSPS,PDR of SAODV, SAOMDV decreases.

Following table 2 shows the performance comparison of SAODV, SAOMDV, SRSSSP and CSSPS protocol in terms of packet loss ratio, end to end delay, throughput, normalized routing load and packet delivery ratio.

**Table2 Comparison of SAODV, SAOMDV, SRSSSP and CSSPS for random topology**

| | PLR | Delay | Throughput | NRL | PDR |
|---|---|---|---|---|---|
| SAODV | 90% | 10 | 58% | 12 % | 91% |
| SAOMDV | 90% | 10 | 73% | 7% | 91% |
| SRSSSP | 60% | 10 | 71% | 5% | 94% |
| CSSPS | 50% | 0 | 82% | 4% | 95% |

## V. CONCLUSION

popularity of proposed art work is to offer strong direction yet however offer protection to the multipath directing information using diverse publications. The art work is foreseeing use modified in particular named on intrigue Separation Vector (MAODV) expertise. MAODV is the satisfactory sensible for UWB MANET. For secure transmission diverse techniques are used, as an example, hash based totally message digest. Reenactment consequences famous propelled imprint based totally coordinating plays excellent besides they are becoming for notably thick frameworks. Proposed sknowknowledge beats with appreciate to throughput, package Conveyance volume and boundaries all of the manner deferral and group trouble quantity.

## REFERENCES

1. NidhiLal, "Acknowledgment of threatening center factor lead via techniques for I-Wathdog information in MANET with DSDV guiding association", science Direct, Procedia software program program designing forty nine (2015) 264 – 273.
2. Mr. Suketu D Nayak and Prof. Sunil J. Soni, "Confirming AODV for MANETs using Message Condensation with thriller Key", January 2011, https://www.researchgate.net/appropriation/261437510.
3. SUPERMAN: safety the usage of past coordinating for compact off the cuff frameworks IEEE trade on flexible Registering 2016.
4. Ali Mohamed E. Ejmaa1, (element, IEEE), " Neighbor-based absolutely unique Availability component guidance convention for portable especially extraordinary device," IEEE get entry to 10, Vol No. four, pp. 8053-8064, June 2016.
5. Xin Ming Zhang. walk, "Neighbor consideration based probabilistic rebroadcast for decreasing coordinating overhead in compact adhoc frameworks", the second one Australian records protection The government assembly 2004 (InfoSec 2004) November 2004.
6. BanothRajkumar, Dr. G. Narsimha, "agree with primarily based statement Denial for cozy Directing in MANET",2d international meeting on Astute Registering, Correspondence and meeting (ICCC-2016), pp. 431-444, April 2016.
7. AnujRanaa, VinayRanab, Sandeep Gupta, "EMAODV: method to anticipate Collective attacks in MANET", fourth worldwide assembly on Eco-32012fd371b2d8bbf6e5e631dc96cdaf Processing and Correspondence Frameworks, ICECCS 2015, October 2015.
8. Todd R. Andel, Alec Yasinsac, "affiliation Dependability and electricity aware Directing convention in Circulated remote structures", IEEE trades on parallel and appropriated shape, vol. 23, NO. 4, April 2012.
9. Charles E. Perkins and Elizabeth M. Royer, "KNN Inquiry planning structures in MANET", IEEE Exchanges ON flexible Figuring, Vol. No. 13, No. 5, also can 2014.
10. Anirudhha Bhattacharya, "one-of-a-kind kinds of strikes in versatile ADHOC gadget: Aversion and assist strategies", branch of technological bdd5b54adb3c84011c7516ef3ab47e54 and constructing basis of Designing, Saltlake, http://www.doc88.com/p-410724870368.html.
11. Arvind Dhaka, "lessen and darkish hollow attack identification using manage Parcels in MANETs", Elsevier, 11th global Multi-gathering on records making ready 2015 (IMCIP-2015) Feburary 2015.
12. "Execution evaluation of AODV with Blackhole assault", global collecting strategies and fashions in technological bdd5b54adb3c84011c7516ef3ab47e54 and Innovation, 2010.
13. RutujiJahavri, "DOS attacks in portable particularly delegated systems", 2nd global assembling on reducing side Registering and Correspondence advancements, 2012 IEEE.
14. Li-Na Weng, Jie Yang "A move-layer soundness primarily based coordinating

framework for extremely wideband frameworks", computer Interchanges 33 (2010) 2185–2194

15. Arathy ok S, S Minesh C N, "An Epic tool for region of unmarried and network organized dark hollow attacks in MANET", worldwide Colloquium in Ongoing Headway and good enough Inquires approximately in building, science and technology(RAEREST2016) technological bdd5b54adb3c84011c7516ef3ab47e54 Direct.
16. Djamel DJENOURI, Nadjib BADACHE, "An research on protection issues in flexible specifically sure systems", February 2004, Labs des, systems informatiques.
17. Ajay Jadhav and Eric E. Johnson, Senior detail, IEEE, "cozy community Directing conference", paper 941.
18. Mike Burmester, aspect, IEEE, Breno de Medeiros detail, IEEE, "On the safety of route Revelation in MANETs", IEEE Exchanges ON flexible Processing, true duplicate had been given April 26, 2007; refreshed stroll 1, 2008.
19. Pawan Kumar Sharma, Vishnu Sharma, "evaluation On safety troubles In MANET Wormhole place and Anticipation", not unusual gathering on Registering, Correspondence and Robotization (ICCCA2016), ISBN: 978-1-5090-1666-2/sixteen/$31.00 2016 IEEE.