International Journal of Reconfigurable and Embedded Systems (IJRES)
Vol. 5, No. 3, November 2016, pp. 153~159
ISSN: 2089-4864

Hardware Implementation of Intrusion detection system for Ad-Hoc Network

M. Reji, P.C. Kishore Raja, Christeena Joseph, Radhika Baskar
Electronics and Communication Engineering Department, Saveetha University, Chennai, India

Article Info

Article history:

Received Apr 24, 2016
Revised Aug 3, 2016
Accepted Aug 18, 2016

Keyword:

Ad-hoc network
AODV
hardware implementation
Microcontroller
Routing Protocol
Zigbee

ABSTRACT

New technologies have been developed in wireless adhoc network need more security. To widespread the adhoc networks we turn in the attention of wireless hand held device mobile phones communicate with short distance using wireless lan card or Bluetooth. The performance of mobile phone are improved greatly for last few years .so security is more important for mobile networks In this paper hardware implementation of single hop ad-hoc network is implemented and analysed using microcontroller. The protocol implemented in this paper is primarily based on, Ad hoc On-Demand Distance Vector routing. We adopt On Demand Distance Vector routing solely based on source routing and "On Demand" process, so each packet does not have to transmit any periodic routing information. We implemented intrusion detection system with five different nodes and the performance parameters like packet delivery ratio, throughput, delay are computed with attacker and without attacker and on demand distance vector routing protocols is proposed to implement in hardware using Zigbee.

Corresponding Author:

M. Reji,
Electronics and Communication Engineering Department,
Saveetha University, Chennai, India.
Email: rejime@gmail.com

1. INTRODUCTION

With the appearance of remote systems, the uses of MANETs [1] are boundless from pursuit and salvage operations to individual region systems. Such applications are portrayed by the absence of interchanges framework and focal power. At the same time frequently the nature of administration or the security of the information must be traded off. These properties make MANET very appropriate in numerous fields [2], as in a war zone, salvage operations and individual region systems.

2. RELATED WORKS

In this area we survey the current secure directing conventions. There exist numerous protected directing conventions in MANET. These protected conventions can't alleviate a wide range of assault confronted by MANET systems. These conventions are more subjected in distinguishing and disposing of certain class of assaults. These conventions while moderating assaults corrupt the QoS of the system to a huge degree. This inadequacy requests a more secure convention, which can alleviate dominant part of the assaults, such that the QoS is not affected. Sanzgiri et.al [7] has proposed Authenticated Routing for Ad hoc Networks (ARAN), which utilizes lopsided cryptography. Since, it utilizes open key encryption secrecy is ensured and system structure is not uncovered. Despite the fact that the convention keeps up a high PDF, it requires additional memory, alongside high handling overhead for encryption. It is still defenseless against assaults such as a dark gap, wormhole and hurrying assaults. Zapta et.al [8] have proposed Secure-AODV (SAODV), which utilizes computerized marks to confirm non-changeable fields of the directing control

messages and one-way hash chains, subsequently securing jump number data. The convention isstrong against assaults such as Dos and Black-opening. Be that as it ay, there are potential outcomes of MIM [9] assaults by trespasser hubs. Papadimitratos et.al has proposed SRP, which keeps up a security relationship in the middle of the source and the destination. It can avert manufacture and circles made by malignant hubs. Be that as it may, it experiences reserve harming and wormhole assaults. Wan et.al has displayed a convention (UBSOR-Unobservable Secure on-Demand Routing Protocol) which accomplishes high protection in receptive steering. It shrouds the substance of the bundles by encryption techniques. In any case, it needs outsiders to build up the key, and can't deal with wormhole assaults.

Li et.al [10] have proposed a Trusted AODV (TAODV) steering convention. It utilizes trust suggestion and later on consolidating these to determine a legitimate conclusion. It trades, trust by means of two bundles called TREQ and TREP, which is an additional overhead. The computational overhead of every validation operation is high, and it might even prompt high activity when there are numerous noxious hubs. Saha et.al [11] have proposed a directing convention, which depends on the idea of loyalty. Devotion is a whole number that is connected with every hub. The methodology lessens the computational overhead to a great deal degree. Be that as it may, the convention can't manage shakedown assaults, nor would it be able to manage grey hole assault successfully. It requires investment to identify and dispense with a vindictive hub from the system. Dhurandher et.al have introduced a convention (FACES-Friend-Based Routing Protocol) which decides trust of the hubs by sending difficulties and sharing companions' rundowns. Difficulties are sent to validate the hubs, and as needs be they are set in companion rundown or question mark list. Companions are appraised on the premise of the measure of information they transmit and rating got from different companions. In any case, it neglects to battle wormhole or hurrying assaults. In addition, the control overhead is expanded because of occasional flooding of test parcel, and intermittent sharing of companion rundown.

3. DESIGN AND DEVELOPMENT

Our aim is to give a protected, dependable and ease equipment convention for MANETs. This gets executed through devotion. A second level of dependability is gotten through suggestions and report bundles. This recognizes the noxious nodes, as well as dispose of them from the system. Subsequently, keeping up a decent QoS for the system. Our fundamental objective of the convention is to construct an ease MANET, which is utilized viably and inexpensively, in a secured way; both in fields such as safeguard and residential.

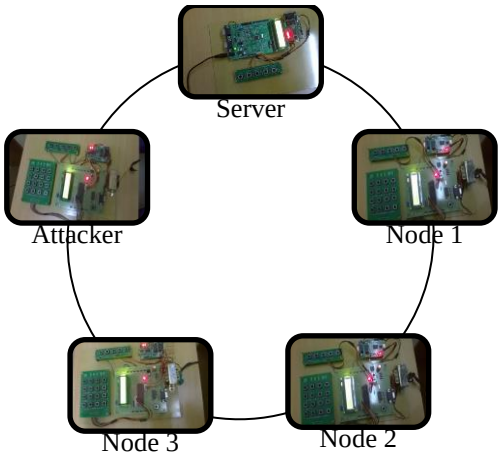

Figure 1. Block Diagram

The components used in making the server and nodes are liquid crystal display (LCD), keypad, microcontroller, ZIGBEE, ARM processor and Analog to digital converter (ADC). The information is transferred from server to the nodes. Where the attacker node or hacker node affects the information sent. Therefore, there is a reduction in the packet delivery ratio (PDR) and increase in average delay time. In case of absence of attacker node we find that there is an increase in packet delivery ratio (PDR) and also decrease in average delay time. Unicast routing protocols is implemented in routing process. Five nodes along with server and attacker is included in this routing process

Algorithm

1. Node 3 needs a route to server.
2. Creates a route request RREQ, then include node server IP address, sequence, enter node IP address sequential hop count=0
3. Node 3 broadcasts RREQ to neighbours
4. Node 2 receives RREQ make a severe route entry for server .next node 4, next hop, hop count 1.
5. Node 2 receivers RREQ.
6. Node 4 receivers RREQ it drops all packets
7. Makes a reverse route entry for node 4 next hop node 2 hop count 1, node 2 receives RREQ.
8. To determine whether the path known to an intermediate node in more recent destination sequences number are used.
9. Node 1 receives RREP.
10. Node 1 receives RREP.
11. Makes a forward route entry for server unicast RREP from node 1 [RREP contains Source and destination]if not node is treated as attacker node
12. Node 1 creates a route reply
13. Unicast RREP to node 1.
14. A node may receive multiple RREP for a given destination from more than one neighbour.
15. The node only forwards the first RREP to receivers.

4. EXPERIMENTAL RESULTS

We have recreated the convention on the equipment, with every one of the transmitters fitting in with the same PAN ID. While setting up the ZigBee modules it is to be remembered that every one of the hubs must fit in with the same system ID, generally the handset won't identify any signs from alternate hubs. We have taken the id of the node as 1, 2 and so on, yet it can be taken as the IP location of the hubs.

In our re-enactment, we have considered that one and only hub is sending information and one hub is getting information, alternate hubs go about as a steering hub. Basic cryptographic images are utilized as a part of the steering calculation, which can be specially crafted by utilization of the system. Hubs move in a 50*26 meter locale, with every hub's transmission range as 15m.

In the principal re-enactment, we consider three nodes. The destination hub is not in the source's extent, so the source sends a solicitation to the closest middle hub, i.e., Node 1. NODE 1 finds the destination hub in its neighbour table, and sends the solicitation straightforwardly. The destination answers, which is sent back to the hub. After, the source hub has gotten the ACK, it builds the devotion of Node 1 by one. Hub 1, does not expand the devotion of the destination hub, since it has been accepted that the destination hub is non-malignant.

Packet delivery ratio

Table 1. Shows packet delivery ratio

No of packets send	With attacker (bits/secs)	Without attacker (bits/secs)
100	73	89
200	70	93
300	68	95
400	64	96
500	60	97

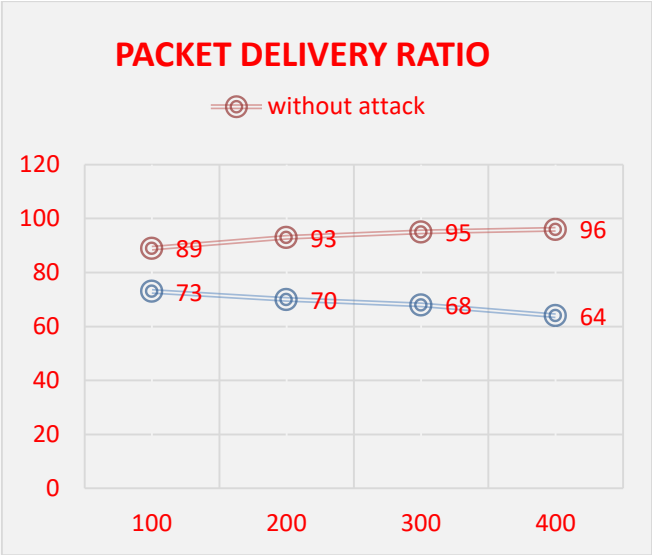

Figure 2. Experimental result for PDR

Average delay time

Table 2. Shows average delay time

No of packets send	With attacker (ms)	Without attacker (ms)
100	100	100
200	120	75
300	180	68
400	208	58
500	300	50

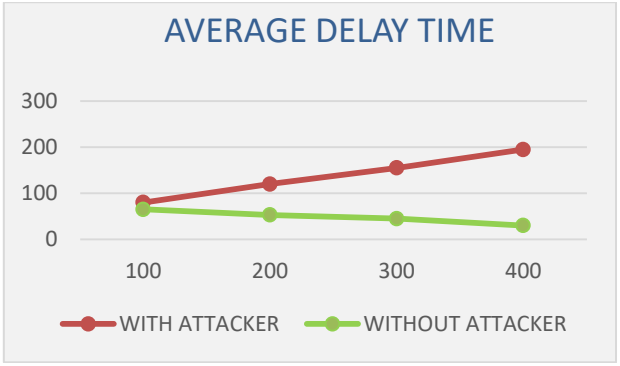

Figure 3. Experimental result for Average Delay Time

In the following recreation, we consider four nodes. The source hub now has two neighbour hubs. Since, Node 2 has constancy zero, the source sends the solicitation to the destination through Node 1. After the source hub gets an answer from the destination, it advances the information from the same course. Give us a chance to assume that Node 1 is a noxious hub, with greyhole assault; then it will drop the ACK bundle rolling in from the destination hub. After the sitting tight time for the source hub is over, it decreases the constancy of Node 1 by one. The server sends a course demand to Node 2, sends the information effectively and its devotion is expanded by one.

5. RESULTS

A broad recreation model having situation of 5 versatile NODE is utilized to think about between layer collaborations with a territory of 50 meter x 26 meter, with every NODE's extent as 15 m. We have considered Node 1 as the source and Node 3 as the destination node. We change the quantity of NODE from 2 to 4, with the portability model as an irregular waypoint model. The normal rate is 1 m/s with respite time of 30 seconds.

At the point when each of the 5 NODES begin steering and couple of transmissions have occurred, the hubs 2, 3, 4are made malevolent, and they begin their assault in a steady progression. We have adjusted the positions of the middle NODE haphazardly and taken the normal estimation of all such hub situations. The same situation has been likewise utilized for execution 46 Hardware Implementation of Fidelity in light of Demand Routing Protocol in Manet's assessment of other secure conventions with which our convention has been analyzed i.e. ARAN, SAODV, TAODV. We consider these conventions as they are surely understood among the safe on interest directing conventions. Additionally, we attempt to demonstrate that our convention stands route superior to the next secured convention.

In the first place, we figure the parcel conveyance portion (PDF) for every one of the conventions. The chart demonstrates that FBOD demonstrates a normal PDF of 89.6%, which is diminished to 83.25% in vindictive environment. Other convention demonstrates vacillations in benevolent and fall in a malignant domain, since none can dispense with the malevolent hubs.

Second, we figure the standardized steering load (NRL) for the conventions as appeared in Figure 20, 21. In the kindhearted environment, the normal NRL for FBOD convention is 0.82, which increments to 1.05 in malignant environment. TAODV indicates high NRL, because of its additional parcels to assemble trust. SAODV and ARAN similarly demonstrates normal NRL, since with incorporation of pernicious hubs parcel of confirmation procedure needs to occur. If there should be an occurrence of FBOD, however constancy it quantifies the trust of the neighbour, and also takes out these pernicious hubs from the system.

Figure 4. Delay time

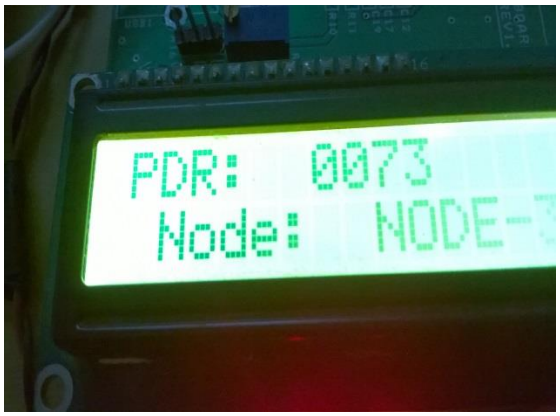

Figure 5. PDR result

Figure 6. Without bad node

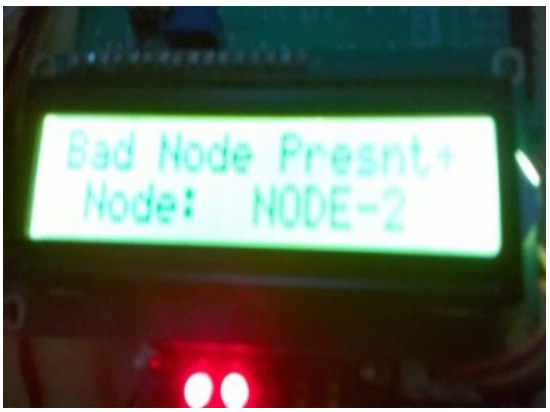

Figure 7. With bad node

At long last, we figure the end to end delay for the conventions in kind hearted environment as appeared in Figure. As the quantity of hubs build, the end to end delay increments. Our convention demonstrates a normal deferral of 15.2 sec in kind and 20.9 sec in malevolent environment. Our convention demonstrates a littler increment at last to end delay, contrasted with other convention, since we can successfully identify and dispose of pernicious hubs, there taking the system back to steadiness. Also, we don't utilize substantial parcels like TAODV, or overwhelming validation plans like SAODV and ARAN, which builds the deferral.

6. CONCLUSION

Our proposed model has numerous interesting components which makes it stand not quite the same as other existing secure on-interest conventions. AODV is a lightweight convention and doesn't require any flooding of additional bundles or additional memory, which is not in the situation of TAODV and ARAN. Also, it is a unicast convention, in this manner making the system free from numerous assaults. The safe course determination mitigates assaults like wormhole and surging assault, which is not in the situation of SAODV. As the constancy of different hubs builds the odds of black hole hub getting chose will diminish. In addition, the tally esteem screens the grey hole and extortion assaults effectively. In our convention, devotion parameter guarantees that just reliable hubs are available in the system. The utilization of the bustling hold up keeps the cycling of RREQ parcels. Parcels like report and proposal help in rapidly distinguishing pernicious hubs and killing them from the system. Once the vindictive hubs are killed, the NRL diminishes back to that on account of amiable environment. We can have watched that our equipment execution works preferred in malevolent environment over other well-known secure steering conventions, with high PDF, low NRL and normal End-to-End delay; thus making it economically practical.

REFERENCES

[1] S. Corson andz J. Macker, "Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations", Network Working Group, RFC: 2501, January 1999.
[2] M. Frodigh, P. Johansson and P. Larsson, "Wireless ad hoc networking: the art of networking without a network", *Ericsson Review*, No. 4, pp. 248-263, 2000.
[3] K. Komali, V. Mahesh and R.Y. Kumar, "A novel secured protocol for data transmission in ad hoc networks using clustering", *International Journal of Computer Science and Information Technologies (IJCSIT)*, Vol. 5(5), pp. 6567-6571, 2014.
[4] S. Sharmila1, G. Umamaheshwari and M. Ruckshana,"Hardware implementation of secure aodv for wireless sensor networks", *ICTACT Journal on Communication Technology*, Vol.1, Issue 04, pp. 218-229, December 2010.
[5] S. Dalu, M.K. Naskar and C.K. Sarkar,"Implementation of a topology control algorithm for manets using nomadic community mobility model", Industrial and Information Systems, pp. 1-5, 2008.
[6] A. Passarella and F. Delmastro, Multi-hop Ad hoc Networks from Theory to Reality, Nova Science Publishers, ch. 9, 2007, pp. 153-177.
[7] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields and E.M. Belding-Royer, "*A secure routing protocol for ad hoc networks*", In: Proceedings of 10th IEEE International Conference on Network Protocols (ICNP), pp.78-87, November 2002.
[8] M. Zapata and N. Asokan, "*Securing ad hoc routing protocols*", In: Proceedings of the 1st ACM Workshop on Wireless Security (WiSe), pp.1-10, September 2002.
[9] R.K. Guha, F. Zeeshan and M. Shahabuddin, *"Discovering man-in-the-middle attacks in authentication protocols"*, Military Communications Conference, MILCOM IEEE, pp 29-31, October 2007.
[10] R.K. Nekkanti and C.W. Lee, "*Trust based adaptive on demand ad hoc routing protocol*", In: Proceedings of the 42nd Annual Southeast Regional Conference, pp 88–93, 2004.
[11] H.N. Saha, D. Bhattacharyya, P.K. Banerjee,"Fidelity based on demand secure (FBOD) routing in mobile adhoc network", Advances in Parallel Distributed Computing, Springer Berlin Heidelberg, pp 615-627, 2011.