ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Elimination of Colluding Insider Selective Forwarding Attacks in Wireless Mesh Network through Forward Monitoring Based Assessment Mechanism (FMAM)

Rachna Beniwal[1], Nisha Pandey[2],

M. Tech Student, Department of CSE & Shri Ram College of Engg. & Mgmt, Palwal, Haryana, India [1]

Asst. Professor**,** Department of CSE & Shri Ram College of Engg. & Mgmt, Palwal, Haryana, India [2]

ABSTRACT: Recently, Wireless Mesh Networks (WMNs) are evolving as an interesting field. WMNs offer technology for next generation wireless networking to offer facilities that are not supported by other Wireless Network. WMNs are mostly deployed in hostile atmosphere where these are un-existed. So WMNs are susceptible to various kinds of security attacks i.e. black hole attack, wormhole, Sybil attack etc. So security is major concern in WMNs. In this paper most critical attack called selective forwarding attack is inquired. In this attack a malicious node discards all or some of obtained packets. An algorithm is described to secure WMNs against selective forwarding attack which depends on FAME. The performance is measured in terms of average end to end delay and throughput. Simulation results have been offered to show the efficiency of the introduced algorithm.

KEYWORDS: Wireless Mesh networks, Route reply packet, Selective forwarding attacks, Detection threshold, FAME

I. INTRODUCTION

In current years, wireless mesh networks (WMNs) obtained much care and proceed to research. Further new services and applications involve health and medical systems, public safety and security surveillance systems, broadband and wireless home internet access and networking disaster and so on. [1]. WMNs contains two-tier architecture, in the first architecture is built up of wireless mesh routers (WMRs) which are normally PowerPC and Advance Risc Machines(ARM) and these mesh routers building a self-organized backbone. Mesh routers are robust with respect to computation and seamless power supply and have communication ability. In second layer, it contains wireless mesh clients (WMCs), which are generally end-user terminals. WMRs behave as a APs (access point), APs requires to be linked with a static internet infrastructure to provide connectivity. APs offer the connectivity to any authenticated WMC. Security is always a significant phase to maintain WMNs. It is enforcing with some encryption algorithms for tunneling i.e. IPSec to offer the safe virtual path along the shared networks. But still WMNs lack effective and scalable security solutions because their security is simple to compromise because of nodes in the shared wireless channel, absence of appropriate infrastructure and dynamic change of configuration. The key management is one of the most significant tasks for networks security. The key technique becomes complicated for WMNs, because there is no authorized third party, no central management. A self-organized was introduced to distribute and maintain the security keys. In this, certificates are recorded and disseminate among themselves.

Wireless Mesh Network (WMN) is the most efficient technology utilized in third generation wireless networking. WMN contains a huge no. of nodes known as mesh nodes and mesh routers which interact via wireless medium and transfer information or data. The no. of network nodes can change from hundreds to thousands. The mesh nodes are static and mesh routers build network backbone. Packet switching is utilized in these networks and data is transferred in the packets form. There are always greater than one data routes or paths are existed between the receiver and sender. Thus routing plays a significant role in the whole network. To support end to end interaction routing protocols are needed. Mesh networks may include either static or mobile devices. WMN networks are utilized in diverse communication requirements, for instance in difficult atmosphere i.e. tunnels, emergency situations, battlefield

DOI: 10.15680/IJIRCCE.2016. 0406340

surveillance, oil rigs etc. A significant possible application for wireless mesh networks is voice over Internet Protocol (VoIP). By utilizing a Quality of Service strategy, the wireless mesh may support local telephone calls to be routed via the mesh. So WMNs are mostly deployed in such circumstances where it is possible for the antagonist or intruder to take control of one or more network nodes. Because of this WMNs are susceptible to several kinds of attacks and selective forwarding attack is most complicated to determine from them.

II. SELECTIVE FORWARDING ATTACK

Forwarding attack is one of many possible attacks in WMN. In this attack, a malicious node forwards a forged Route Reply packet (RREP) to a source node that starts the route discovery for pretending to be a target node. When a source node obtained numerous RREP then by comparing the destination sequence number (describes an up-to-date path to a destination) contained in every RREP packets it detects the highest one as the most recent routing information and chooses the route contained in that RREP packet. In case the sequence no. are equal it chooses the route with the minimum hop count. If the intruder spoofed the identity to be the target node and forwards RREP with destination sequence no. greater than the actual target node to the source node, the data traffic will flow toward the intruder. Thus, source and target nodes become unable to interact with one another.

A forwarding node can also forward a response to a route request (RREQ) message from any source in the network which indicates the node itself is a closest node to the destination node and obtain all the packet of data meant for some other node from the source node.

In forwarding attack malicious node acts like gray hole or the black hole. In black hole attack malicious node denies to send all packets and simply discards them, assuring that they are not propagated any further. Since, such an intruder runs the risks that neighboring nodes will conclude that intruder node has failed and decide to see another route. A more difficult form of this attack is gray hole attack in which a malicious node selectively sends packets. An antagonist interested in suppressing or changing packets created from a few chosen nodes can flexibly send the remaining traffic and decreases suspicion of wrong doing because some packets are also discarded because of channel losses and increased congestion with traffic increment. In such scenario it becomes very complicated to determine an intruder in the WMN networks.

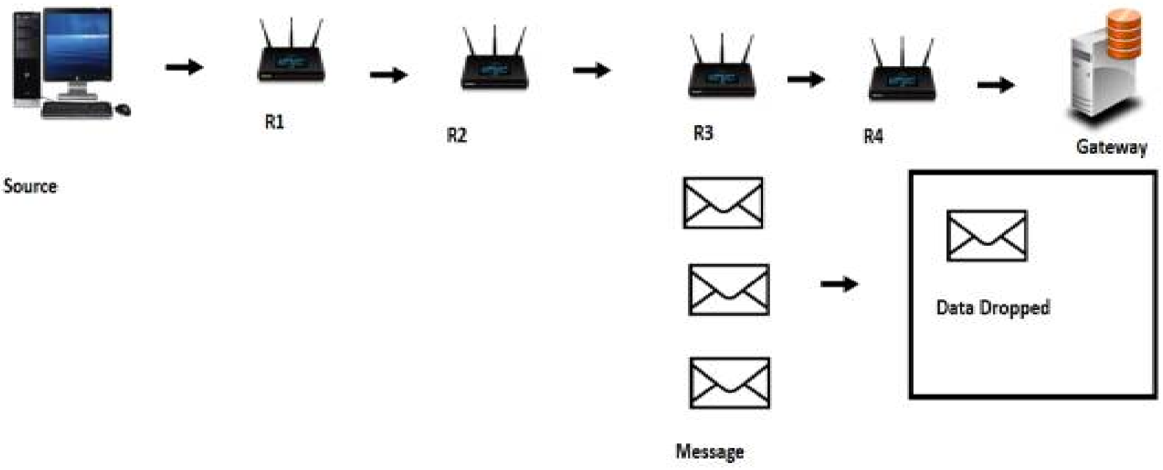

Figure 1: Selective Forwarding attack

How Forwarding affects WMNs

In fig1 it is depicted that in Ad Hoc On-Demand Distance Vector (AODV) routing network the malicious node “A” first determines the active route in between the forwarder “E” and target node “B”. The malicious node “A” then forward the RREP to node "C" which has the spoofed destination address of node "B" involving minimum hop count and large sequence no. Then node “C” sends this RREP to the forwarding node “E”. Now this route is utilized by the sender to forward the data and in this manner data will reach at the malicious node "A" rather than correct node "B".

DOI: 10.15680/IJIRCCE.2016. 0406340

When malicious node "A" obtains data from node "C" it will discard some data and rest of data will be forwarded to target node "B". In this way forwarder and destination node will be in no position to interact accurately in state of selective forwarding attack. This kind of attack mostly occurs in border area, where it becomes complicated to determine enemy movement across the border and a country can also loss a war.

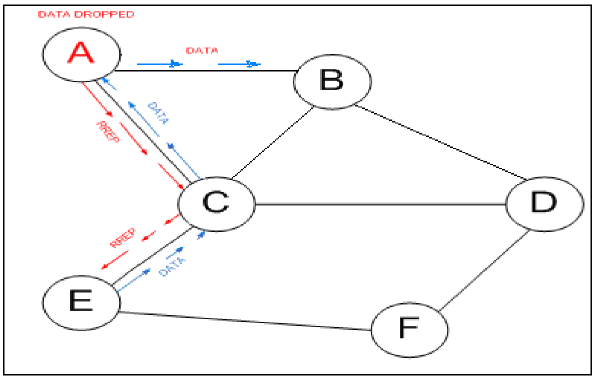

Fig. 2 Selective forwarding attack specification

III. SECURITY ATTACKS IN WMNs

Security attacks are based on the several factors. It is based on the behavior, nature or the protocols that are utilized on the several layers. Moreover, the attacks can be categorize, depending on the attacker method to utilize to achieve their motive, is on fabrication, impersonation, modification, Denial of Service (DoS) and other attacks. Glass et. al. in explain the attacks at the various layers of WMN protocol stack is described (in Table I).

A. Security Attacks at the Physical Layer of WMNs

There are several kinds of attacks at the first physical layer of WMNs. An intruder may damage the external hardware, simply routers are installed at the external region. Such routers are sensible, an intruder can easily extract the information from them. The periodic jamming, trivial jamming, reactive jamming attacks are may be used in the physical layer [9]. In trivial jamming attack, attacker transfers the noise seamlessly. In periodic jamming attack (or scrambling attack), an intruder forwards a short signal periodically. In last reactive jamming attack, whenever an intruder determines that a node has started a transmission, an attacker transfers a signal.

B. Security Attacks at the MAC Layer of WMNs

Several attacks are possible at WMNs MAC layer and these consist of:

1) Passive Eavesdropping: The behavior of the WMNs is flooding the transmission, it is possible for intruder to launch the passive eaves dropping within the transmission range of the communication nodes. It can be launched in external as well as internal nodes. In internal eavesdropping by the malicious intermediary nodes hold the copy of data and send to any network nodes without information [6].

2) Flooding Attack: An attacker forwards several MAC control messages to its neighboring nodes. Because of this, the medium fairness is physically abused [10].

3) MAC Spoofing: An attacker attempts to change the MAC address during frames transmission.

4) Jamming Attack: Jamming attacks are also possible at MAC layer. Seth and Gankotiya [9] assume some jamming attacks, and these are unprompted reactive request to send (RTS) jamming attack, clear to send (CTS) attack and CTS corrupt jamming. In CTS corrupt jamming, based on the receipt RTS, an attacker transfers noise during the CTS reply. In RTS jamming attack, whenever attacker determines the RTS message, it interrupts the RTS message by immediately initiating of a transmission.

C. Security Attacks at the Network Layer of WMNs

Various attacks are also possible at the network layer. These attacks are further classified into two groups:

1) Control Plane Control Plane or (routing) concentrate on the routing services of the network. The Control Plane attacks are differentiated as below:

2) Rushing Attacks: In on-demand routing protocols, an intruder forwards several routing packets across the network in a short interval of time for holding nodes busy.

3) Routing Table Overflow: An attacker tries to determine routes to imaginary nodes with motive to generate enough routes to avoid new routes from being generated.

4) Wormhole Attack: In this attack, intruder convince the nodes to utilize the malicious path and if two or more malicious nodes collude together during this by setting up a tunnel. A wormhole attack utilizing an effective communication medium. Once, the victim node enters the malicious nodes in the routing path, the malicious nodes begins dropping packets.

5) Sinkhole (or Blackhole) Attack: In this attack, a malicious node initiates convincing to its neighboring nodes for sending packets. That is the “most optimal” node for sending the packets. When a neighbor node starts to send the packet, then malicious node discards the packets which are sent by the neighboring nodes.

6) Greyhole Attack: A grey hole attack is a version of sinkhole attack [5]. During this attack, they will not lost all the packets but they just drop the particular packets [9].

7) Location Disclosure Attack: During this attack, it reveals the information or structure about the nodes location in the network [14].

8) Data Control Attacks: Data control plane (or path forwarding) attacks target path forwarding services of the network. These kinds of attacks are established by misbehaving nodes in the network. Bansal et. al.[15] classified into two groups: malicious nodes and selfish nodes. A selfish node is concerned about its performance even at the operating cost of other nodes, while a greedy node attempts to interfere the operation of network. The simple manner is to control the attack is eavesdropping.

D. Security Attacks at the Transport Layer of WMNs

An intruder could target the transport layer. The possible attacks at the transport layer are desynchronization and flooding. In the flooding attack, a malicious node may build new connection requests for resources needs arrive a maximum limit. In desynchronization attack, a malicious node may repeatedly spoof the messages, so that host to request the retransmission of missed frames.

E. Security Attacks at the Application Layer of WMNs: This layer attacks are only concern with the malicious codes, virus, worms, application abuses etc. in the wireless networks.

IV. SOLUTION METHODOLOGY

We introduced an algorithm to design an intrusion detection system to determine the forwarding attack in WMNs by building usage of two factors i.e. number of packets and send packet delivery ratio based on loss, delay and required data rate. This detection system depends on FAME. FAME offers a definite conclusion depending on noisy or missing input information. The performance is measured in terms of average end to end delay and throughput.

First we set three thresholds levels high, medium and low which describe the dropped packets among nodes. These dropped packets involve the loss rate because of the increased traffic and channel losses in the network. The performance of every node is measured in the network from source node to destination node. Low and medium levels describe that the network is good for interaction and high level describes a weak connection. Every level shows different loss rates through the usage of priorities.

When it is adjusted that no antagonist is available in the network then we examine for false alarms and optimal path from source node to destination node because in mesh network there is always more than path available between source node and destination nodes. In this step every node which behaves as router is examined for condition to obtain the best results. For identifying the best neighbor node we analyze the three parameters lost packets, required rate and last packet time. Lost packets describe the number of lost packets, expected rate describes the number of expected packets to be obtained at the recipient side and last packet time is utilized to compute the time of last packet of stream obtained at the recipient side which shows the communication path delay. By utilizing these three parameters we adjust the priorities. When lost packet is low, expected rate is high and last packet time is low situations are better for data transmission and priority is high. When lost packet is medium, expected rate is medium and last packet time is medium then priority is medium. When lost packet is high, expected rate is low and last packet time is high then priority is low. A node having optimal conditions is chosen and communication begins. Same tests is done at every node through the transmission route.

V. PROPOSED ALGORITHM

Forward Monitoring Based Assessment Mechanism (FMAM)

The solution that we introduce here is generally only changes the source node working without changing intermediary and destination nodes by utilizing a method known as Prior_Receive Reply. In this technique three things are appended, a new table RR-Table (Request Reply), a timer WT (Waiting Time) and a variable MN-ID (Malicious Node ID) to the data structures in the actual AODV Protocol.

DSN – Destination Sequence Number, NID – Node ID, MN-ID – Malicious Node ID(M node).

Step 1: (Initialization Process) fetch the current time and add the current time with waiting time.

Step 2: (Storing Process) Store all the Route Response DSN and NID in RR-Table(R) table. Replicate the above procedure until the time exceeds.

Step 3: (Identify and Remove Malicious Node) Fetch the first entry from RR-Table, If DSN is much greater than SSN then drop entry from RR-Table and record its NID in MN-ID.

Step 4: (Node Selection Process) Sort the contents of RR-Table entries according to the DSN choose the NID having maximum DSN among RR-table entries.

Step 5: (Continue default process) Call Receive Reply mechanism of default AODV Protocol. The above algorithm initiates from the initialization procedure, first set the waiting time for the source node to obtain the RREQ coming from other nodes and then append the current time with the waiting time. Then in storing procedure, record all the RREQ Destination Sequence No. (DSN) and its Node Id in RR-Table until the calculated time exceeds. Basically the first route response will be from the malicious node with large destination sequence no., which is recorded as the first entry in the RR-Table. Then compare the first destination sequence no. with the source node sequence no., if there available much more differences among them, certainly that node is the malicious node, immediately eliminate that entry from the RR-Table. This is how malicious node is determined and eliminated. Final procedure is choosing the next node id that has the greater destination sequence no., is achieved by sorting the RR-Table according to the DSEQ-NO column, whose packet is forwarded to Receive Reply method for continuing the default operations of AODV protocol. Additionally, the introduced solution manages the malicious node identity as MN-Id, so that in future, it can drop any control messages coming from that node. Now however, malicious node is determined, the routing table for that node is not managed. Additionally, the control messages from the malicious node, too, are not sent in the network. Furthermore, for maintaining freshness the RR-Table is flushed once a route request is selected from it[13]. Hence, the operation of the introduced protocol is similar to original AODV, once the malicious node has been determined.

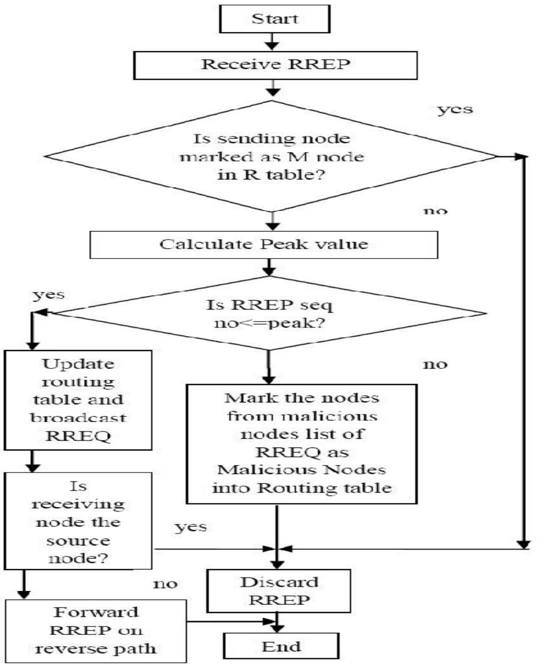
Start
Receive RREP
yes
Is sending node marked as M node in R table?
no
Calculate Peak value
yes
Is RREP seq no<=peak?
no
Update routing table and broadcast RREQ
Mark the nodes from malicious nodes list of RREQ as Malicious Nodes into Routing table
Is receiving node the source node?
yes
no
Discard RREP
Forward RREP on reverse path
End

Figure 3: Proposed Algorithm

IV. PERFORMANCE EVALUATION

The introduced system is implemented in NS2 and system performance is measured in terms of average end to end delay and throughput.

A. Simulation Parameters The network configuration contains a square grid of 36 mesh nodes. In our simulations FTP and UDP are utilized for data transmission. AODV routing protocol is employed for routing between source node and destination node. Packets have a size of 1024 bytes and are forwarded at a deterministic rate.

B. Simulation Analysis From table number1 it is clear that there is importantly increase in the network throughput. Results are also represented utilizing graphs in terms of simulation time.

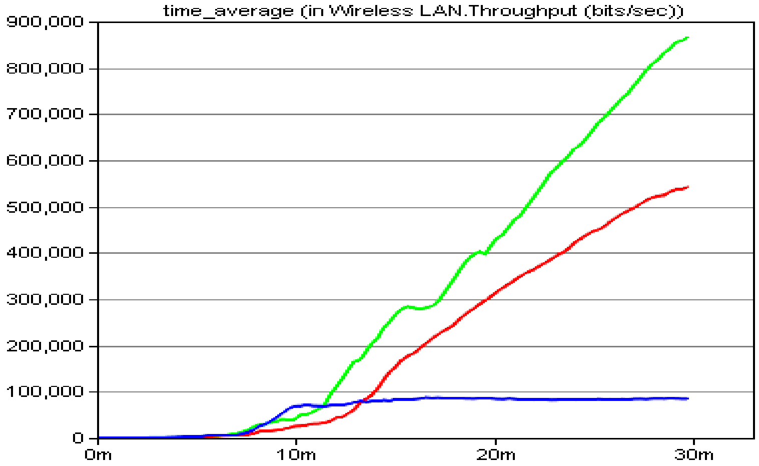

Fig. 4 Throughput versus Simulation Time

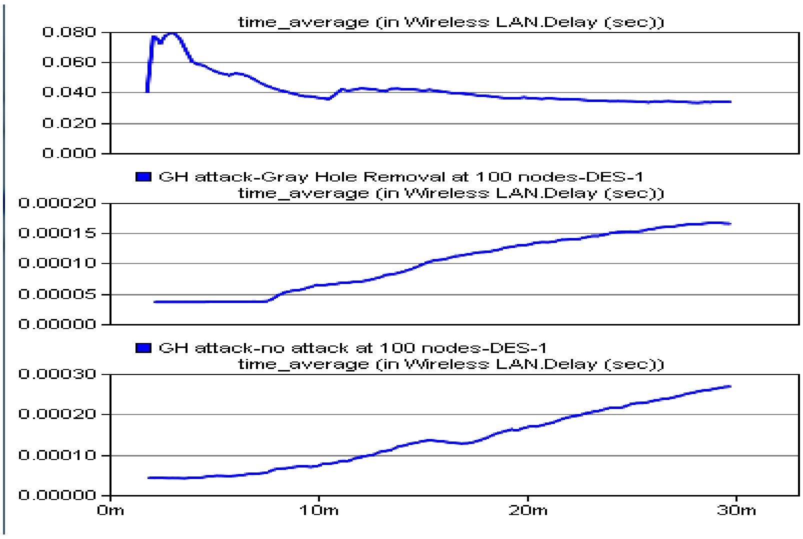

Fig. 5 Average End To End Delay versus Simulation Time

But there is increment in the average end to end delay which is caused by the increase in the nodes complexity and increased amount of network overhead. This average end to end delay can be reduced by increasing the system bandwidth because of which system become costly. By evaluating average end to end delay in advance we can choose the proper system bandwidth which will offer optimal and reliable data delivery.

V. CONCLUSION

In this paper we introduced an algorithm depending on FAME which would secure the network from the selective forwarding attack and this depends on the prioritization technique so that always the less severe nodes will be chosen as the participating node. Introduced system offers a better throughput in hostile atmosphere. Simulation results are utilized to show the efficiency of the introduced system**.** The technique has been simulated utilizing the modeler RIVERBED and results are compared which indicate an important increment in throughput. But there is increment in average end to end delay whose influence can be decreased by increasing the system bandwidth. Hence, the system has successfully protected from the attack and offers a flexible transmission. Further performance can be enhanced by choosing the energy efficient route in condition of AODV protocol so that lifetime of network will be increased.

REFERENCES

[1] Abedi, O.; Berangi, R.; Azgomi, M.A., "Improving Route Stability and Overhead on AODV Routing Protocol and Make it Usable forWireless Sensor Networks," in Proceedings of 29th IEEE International Conference onWireless Sensor Networks,June 2009, pp.464,467.
[2] Chowdhury, S.I.; Won-Il Lee; Youn-Sang Choi; Guen-Young Kee; Jae-Young Pyun, "Performance evaluation of reactive routing protocols inWireless Sensor Networks," in proceeding of Communications (APCC), 2011 17th Asia-Pacific Conference onad hoc networks ,2011, pp.559,564.
[3] C. Gayathri and r. V. Kavitha," Mitigation of Colluding Selective Forwarding Attacks in WMN using FADE", International Journal for trends in Engineering and Technlogy, vol.3, isse 3, jan 2015, ISSN- 2349-9303.
[4] Dr. seema verma, prachi," simulation based routing protocols evaluation for IEEE 802.15.6 enabled WSN",ACEEE int.j. on Network Security, Vol. 2, no. 3, july 2011
[5] Fathima Ameza, N. Assam," Defending AODV Routing Protocol against the Black Hole Attack", International Journal of Computer Science and Information System, vol. 08, issue 2 2010.
[6] Irshad Ullah," Effects of Black Hole Attacks on MANET using Reactive and Proactive Protocol", International Journal of Computer Science, vol.10, issue 3, may 2013.
[7] Jaspreet singh, anuj gupta," mitigating selective forwarding attacks in WSN",international journal of latest trends in engineering and technology, vol.4, issue 2, july 2014, 222- 228
[8] Preeti sharma, monika saluja and krishan kumar saluja," A review of selective forwarding attacks in wireless sensor n/w", international journal of advance smart sensor network system, vol.2, issue 3, july 2012, 37-42
[9] Path M Dave, Purvang D Dalal," simulation and perfomance evaluation of routing protocols in WSN",international journal of advanced research in computer and communication engineering, vol.2, issue 3, march 2014,1403
[10] Surinderjit kaur, amrit kaur, kiranveer kaur," improved secure routing scheme with encrypted session keys in WSN", international journal of emerging research in management and technology, vol.2, issue 3, march 2014, 2278-9359
[11] S. Rajaraman and A. Babu Karuppiah," False Misbehavoiur Elimination of Packet Dropping Attackers during Military Survillance using WSN", Advance in Military Technology, vol.9, issue 1, june 2014.
[12] Yu Hu, Yuanming Wu, Hongshuai Wang," Detection of Insider Selective Forwarding Attack Based on Monitor Node and Trust Mechanism in WSN", Scrip Journal, vol.6, 2014, 237-248.
[13] Vinod Namboodiri, Manish Agarwal, Lixin Gao; "A Study on the Feasibility of Mobile Gateways for Wireless Sensor Networks", in proceeding of Wireless Communications Networking and Mobile Computing 6th International Conference on 2010,Sept. 2010, pp.1,4, 23-25.
[14] Siva D., Abu B. Sesay, and Witold A. Krzymie´n, "A Design on Routing Protocol in Sensor Networks Based on Clustering Optimization" In Proceedings of 2nd International Conference on Future Computer and Communication,2010, pp 473-477.
[15] C. Y. Wan, S. B. Eisenman, and A. T. Campbell,, "CODA: Congestion Detection and Avoidance in Sensor Networks," In Proceedings of FirstACM Conference on Embedded Networked Sensor Systems,2003,pp.266-279.
[16] R.U.Anitha, P. Kamalakkannan ,"Enhanced Cluster Based Routing Protocol for MobileNodes in Wireless Sensor Network" In Proceedings of 2013 International Conference onPattern Recognition, Informatics and Mobile Engineering (PRIME), 2006,PP 187-193.
[17] Samera. B. Awwad, cheekyung and Nor K. Noordin "Cluster Based Routing (CBR) Protocol with Adaptive Scheduling for Mobility and Energy Awareness in Wireless Sensor Network," In Proceedings of Proceedings of the Asia Pacific Advanced Network,2009, pp 34-46.
[18] R. Balasubramaniyan , Dr. M. Chandrasekaran "A New Fuzzy Based Clustering algorithm for Wireless Mobile Ad-Hoc Sensor Networks "In Proceedings of 2013 International Conference on Computer Communication and Informatics,2013, pp 31-37
[19] Stephan Olariu, "Information assurance in wireless sensor networks", Sensor network research group, Old Dominion University, Wireless Communication and Mobile Computing, Vol. 4,No 6,pp.623-637,2009.
[20] Harpreet Singh, Gurpreet Singh Josan, "Performance Analysis of AODV & DSR Routing Protocols in Wireless Sensor Networks", International Journal of Engineering ,Vol. 2, Issue 5,pp,2212-2216, September- October 2012.
[21] Xuanxia Yao, XueFeng Zheng, "A Secure Routing Scheme for Static Wireless Sensor Networks", IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Vol.2, pp.776-780, 2008
[22] Rayala Upendar Rao, "Secure Routing in Cluster based Wireless Sensor Networks using Symmetric Cryptography with Session Keys", International Journal of Computer Applications, Vol. 55, Issue. 7, pp.48-52, October 2012
[23] Fan Li and Yu Wang; " Survey of Routing in Wireless Sensor Networks",in Proceedings ofIEEE Wireless Sensor Networks Technology Magazine, Volume 2, Issue 2, June 2007; pp. 12-22.
[24] Jahanzeb Farooq, Bilal Rauf "Implementation and Evaluation of IEEE 802.11e WirelessLAN in GloMoSim" In Proceeding of the 1st ACM International Workshop on Ad Hoc Networks, NY, USA, 2004,pp. 76-85.
[25] Yue Liu, Jun Bi, Ju Yang; "Research onWireless Sensor Networks"in Proceedings of Chinese Control and Decision Conference (CCDC), 2009, pp.4430 – 4435