International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 9, ISSN No. 2455-2143, Pages 83-89
Published Online July – August 2016 in IJEAST (http://www.ijeast.com)

VARIOUS ROUTING PROTOCOL, ATTACKS AND TYPES OF NETWORK IN MOBILE AD-HOC NETWORK BASED ON WIRELESS SENSOR NETWORK: A REVIEW

Sonia
Computer Science & Engineering
SVIET, Banur, Punjab, India

Harkomalpreet Kaur
Assistant Professor CSE
SVIET, Banur, Punjab, India

Abstract - Wireless sensor network (WSN) contains of a huge amount of sensor nodes. A sensor node is defined as a small, wireless method, skillful of replying to one or a number of stimuli, handling the data and transmitting the information over a small distance by radio frequencies or laser methods. Mobile ad hoc networks (MANETs) are collections of autonomous wireless mobile knobs built dynamically lacking the use of any existing network infrastructure or centralized administration. These grids are suitable for systems in which no infrastructure exists, such as military battlefield, emergency rescue, and vehicular communications. MANET constantly changes over time; the simple use of a static base profile may not represent the current state of the network.

Keywords: Wireless Sensor Network, Mobile ad-hoc network, vehicular communication and approaches.

I. INTRODUCTION

Wireless sensor networks (WSNs) typically comprise a large number of power-constrained sensor units that typically perform multi-hop information communication to a base station (sink). WSNs can be used for a number of requests ranging since surveillance and situation monitoring to health care and military operations. A number of requests need that sensor nodes be leftward unattended for a long period of time due to cost implications or problematic entrée to the arrangement area. Consequently, energy consumption is a major concern when designing protocols for WSNs. Wireless device networks (WSNs) must played an significant character in area of agriculture, surveillance, environment monitoring etc. Knobs which are little in cost are dispersed in explicit area. Data is collected from nodes processed and data is common among several nodes. There is identical fewer infrastructures in used in WSN. WSN consists of large number of nodes which might vary since few thousands to find the information from the setting. [1]

Advantages of WSN

The advantages and disadvantages of wireless device networks can be abridged as surveys:

Advantages:

- Network setups can be done without fixed infrastructure.
- Perfect for the non-reachable spaces such as crossways the sea, mountains, rural areas or deep forests.
- Flexible if here is ad hoc condition when supplementary workstation is mandatory.
- Implementation cost is cheap.
- *Disadvantages:*
- Fewer secure since hackers can arrive the entree point and become all the data.
- Lower speed compared to
- Additional compound to arrange than a bound network.
- Easily affected through surrounds (dividers, heat, large spaces due to sign attenuation, etc.).[2]

II. TYPES OF NETWORK

Wireless sensor networks are deployed on property, under-water, and under-ground. A sensor network faces different challenges and constraints according

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 9, ISSN No. 2455-2143, Pages 83-89
Published Online July – August 2016 in IJEAST (http://www.ijeast.com)

to the situation in the sensor system organized. There are 5 kinds of the wireless sensor network as

1. Wire-less Native sensor Grids.
2. Wire-less Underground sensor Grid network
3. Wire-less Under-water sensor Grids network
4. Wire-less Multi-media sensor Grids network
5. Wire-less Mobile sensor Grids network

- **Terrestrial WSNs** characteristically contain of hundreds to thousands of low-cost device knobs organized in a assumed region, whichever in an ad hoc or in a replanted method. In ad hoc positioning, sensor knobs can be released from a horizontal and randomly located into the board space. In pre-planned positioning, there is net assignment, best placement, 2-d and 3-d assignment replicas. In a terrestrial WSN, dependable communication in a dense situation is very indispensable. Sensor nodes essential remain capable to positively communicate through the base position in terrestrial WSN, though battery control is incomplete. In any case, it is indispensable for sensor nodes to conserve energy.

- **Underground WSNs** in which a bound network Device knob enclosed underground, essentially it used for detects used to monitor underground situation. And bowl knob are used for communicate evidence to the sensor node to the base station. This wireless senor network is supplementary expensive as associate to terrestrial WSN in relationships of equipment, deployment, and maintenance. Underground sensor nodes are luxurious because correct mechanisms must be used for consistent communication through soil, rocks, water, and other mineral fillings. The underground situation types wire-less transmission a challenge due to signal losses and high levels of attenuation [3].

- **Underwater WSNs** contain of a quantity of device knobs and vehicles organized underwater. Unlike terrestrial WSNs, underwater device knobs are supplementary costly and less solid. Independent underwater vehicles are used for searching or gathering information from device nodes. Device nodes transmit through auditory waves in underwater WSN. Acoustic communication is a challenge in submerged due to incomplete bandwidth, extensive propagation delay, and signal fading problem.

- **Multi-media WSNs** are used to checking and following of measures in the form of hypermedia. Multi-media WSNs consist of a number of little cost device nodes armed with cameras and micro-phones. These sensor nodes communicate with each other for information retrieval, procedure, association, and compression over a wireless connection. Multimedia sensor nodes are deployed in a replanted method into the sky for exposure guarantee. High bandwidth demand, high energy consumption, excellence of facility (QoS) disorder, information processing and compressing techniques and cross-layer design are challenges in hypermedia WSNs.

III. MOBILE AD HOC NETWORK IN WIRE-LESS SENSOR NETWORK

Mobile ad-hoc network is a collection of device knobs that could move on their individual and interrelate with the physical environment. Mobile nodes have the ability of detecting, computing, and transmission like stagnant nodes. Important dissimilarity is mobile nodes have the aptitude to alteration the position and establish itself in the grid. Mobile WSNs can start with some initial deployment and nodes can then spread out to gather information. Mobile knob can interconnect to additional mobile node when they are within the range of every other and transmission gathered data. Another important difference is data distribution. In mobile WSNs, data could be dispersed using vibrant routing while secure routing or flooding is used in fixed WSNs. Sensor nodes placement, self-organization, localization, steering and controller, exposure, energy, conservation, and data process are challenges in mobile WSNs[3] . Mobile Ad hoc networks play an important role in today's communication. MANET is a collection of multi hop wire-less mobile knobs, which transfer with every other without Established infrastructure [2]. Since MANET does not require an infrastructure, it can be easily deployed at any place, where setting up an infrastructure is difficult. These networks find wide application in military, vehicular ad hoc networks, civilian environment, disaster area, etc. Each node in MANET is required to act as a host

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 9, ISSN No. 2455-2143, Pages 83-89
Published Online July – August 2016 in IJEAST (http://www.ijeast.com)

as well as a router, which have to forward packets between nodes which cannot directly communicate with each other. Each node in MANET is self-configurable and is responsible for routing and forwarding the packet. This is accomplished by using different routing protocols. [4]

IV. RELATED WORK

Meysam Alikhany et al.,2011[5] proposed clustering-based irregularity detection approach, called DCAD, which allows the shape to be dynamically updated. In the approach, they use the weighted fixed width clustering algorithm in order to originate a normal profile and to detect anomalies. They also use weighted coefficients and a overlooking reckoning to occasionally update the usual profile. They behaviour MANET simulations using the NS2 simulator and consider situations for detecting several types of routing attacks on AODV protocol. **Debdutta Barman Roy et al.,2013**[6] presented novel cluster based interference detection algorithm that takes care of black hole attacks in a MANET. This planned algorithm was based on responsibility of the nodes in a network. The network is measured to be a layered structured. The nodes were associate of a cluster .Each cluster had cluster head that takes care of all the members of its own cluster and interconnects with cluster head at layer 2 whenever required. The cluster head at layer 2 transfer through all cluster crowns at level 1. The assortment of cluster head depends on three parameters battery power, mobility and trust value of a node in a cluster. Sometimes the cluster head updating is done according to three parameters. **Anju J et al.,2014** [4]described a wormhole attack propelled by exploiting AODV protocol in MANET, was perceived and abolished in two phases. The opening phase in the process of identifying wormhole attack was done, based on timing investigation and hop count. After mistrusting the attack, a Clustering based method was used to approve the attendance of occurrence, and also to classify the attacker knobs. The entire network was divided into different clusters and each cluster will have a Cluster Head, which reins all the nodes in the cluster and plays the role of a supervisory authority in MANET. **Jitendra Sayner et al.,2014** [7]addresses security and performance problems of MANET. A novel cluster concerned with concept was proposed to increase security and efficiency of the network. Planned strategy insures the optimal performance of MANET in existence of black hole attack. The imitation of the proposed methodology was carried out using NS2 network simulant and the simulation significances reflect the performance of scheme for detection and deterrence of the black hole. **Md. Zair Hussain et al.,2013** [8]advancement in last period in electronics & communication, computer science and information technology domain had caused in the new computing and communication era, known as Wireless Sensor Networks. The routing protocols vary on the basis of application and network architecture. With consciousness was a required design criterion, many new protocols had been specifically intended for routing, power management and data distribution. Efficient routing in a sensor network necessitates that routing protocol must minimalize network energy dissipation and exploit network lifetime. **Kehkasa Mirza et al, 2015** [9] Wireless Sensor Network is one type of ad-hoc systems; it has imperfect bandwidth, little energy with minor battery. Use of this feature make sensor infeasible to used security solution. It has many requests like military battle field, habitat monitoring, target tracking, seismic monitoring, and fire and flood discovery. One of the most significant attacks in wireless sensor networks is the wormhole attack, in this attack a malevolent node receives packets and massage from one side position and tunnels them to another location in the network. To perceive this types of attack certain wormhole detection techniques can be used like Cluster Based Approach

V. TYPES OF ATTACK IN MANET

Passive attack: In this type of attack, the intruder only performs certain types of monitoring on convinced networks to get info about the traffic devoid of injecting any fake information. This category of violence serves the attacker to improvement info and makes the footprint of the invaded network in order to relate the attack positively. The kinds of passive spasms are eavesdropping, traffic analysis and snooping:

A. *Denial of service attack:* Repudiation of facility spells are meant at complete disruption of routing information and therefore the entire process of ad-hoc net.
B. *Traffic Examination:* In MANETs the information packages as well as circulation design both are significant for opponents. For example, intimate data about grid topology can be derived by analyzing circulation shapes. Traffic analysis could also be lead as active attack by destroying nodes, which stimulates self-organization in

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 9, ISSN No. 2455-2143, Pages 83-89
Published Online July – August 2016 in IJEAST (http://www.ijeast.com)

the system, and valued data around the topology can be gathered. Traffic examination in ad hoc networks may reveal following type of information.

C. *Snooping:* Snooping is unauthorized access to another person's data. It is similar to snooping but is not unavoidably limited to ahead access to data during its transmission. Snooping can comprise casual adherence of an e-mail which seems on another's CPU screen or watching what somebody else is typing. More sophisticated prying usages software packages to remotely observer activity on a computer or network device

Active attack: In this type of violence, the interloper performs real violation on whichever the network resources or the data transmitted; this is complete through International Journal taking place New Computer Manners and Their Applications causing routing disruption, network resource reduction, and node contravention. In the subsequent are the kinds of active attacks over MANET and how the attacker's threat can be performed

A. *Flooding attack:* In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a knob's assets, such as computational and battery-operated power or to interrupt the routing operation to cause severe degradation in system performance. For sample, in AODV protocol, a mischievous node can drive a large number of RREQs in a small epoch to a endpoint node that does not occur in the network. Because no one will reply to the RREQs, these RREQs will overflow the entire network. As a result, all of the knob battery power, as well as network bandwidth will be obsessive and might prime to denial-of-service.

B. *Black hole Attack:* Route discovery process in AODV is vulnerable to the black hole attack. The device, that is, slightly intermediary node may respond to the RREQ message if it has a fresh enough routes, planned to decrease routing delay, is used by the mischievous node to compromise the system. In this attack, when a mischievous node attends to a route appeal packet in the system, it responds with the claim of having the shortest and the freshest way to the endpoint node even if no such path exists. As a result, the malicious node easily misroute network circulation to it and then droplet the packets fleeting to it.

C. *Rushing Attack:* Whistle attacks are mostly in contradiction of the on-demand direction-finding protocols. These types of attacks disrupt the route discovery process. On-demand routing protocols which use identical suppression during the route detection process are vulnerable to this attack. When cooperated node accepts a route appeal packet from the basis node, it floods the packet quickly throughout the network before additional nodes, which similarly receive the similar route request package can respond. For example, in symbol the node "4" signifies the rustle attack knob, where "S" and "D" mentions to basis and endpoint nodes. The rushing attack of cooperated knob "4" quickly transmissions the direction request messages to ensure that the RREQ message from itself arrive previous than fix those since other knots. This result in when neighboring knob of "D" i.e. "7" & "8" later get the real (early) track request from basis, they simply abandon requests. Consequently in the attendance of such attacks "S" flops to discover some useable route or harmless route without the connection of attacker.[10]

VI. DIFFERENCE BETWEEN BLACK HOLE AND GRAY HOLE ATTACK

Black hole Attack	**Gray hole Attack**
▪ When a knob requires a direction to endpoint, it initiates a direction discovery process within the network. In our reproduction we careful the	▪ The Gray Hole attack has two phases. Initially, a mischievous node deeds the AODV protocol to promote itself as consuming a valid route to

case in where the intruder directs fake RREP packets.

- In AODV after receiving a RREQ message, a confidential attacker might forge a RREP communication as if it had a rehabilitated enough way to the destination knob. In order to subdue other sincere RREP messages that the basis knob obtains from additional nodes, the attacker copies a faked RREP communication by accumulative the endpoint sequence amount.
- An attacker might interrupt the route between the target knobs to assumed endpoint, or attack in the route between by suppressing other alternative routes.
- In order to subdue other genuine RREP messages that the basis node might obtain from other knobs, the attacker might copy a faked RREP communication by accumulative the endpoint sequence number. [11]

an endpoint node, with the meaning of interrupting packets, smooth though the direction is spurious.

- Following, the knob drops the interrupted packages with a confident prospect.
- This attack is additional difficult to notice than the dark Whole attack where the mischievous node drops the received data packets with certainty.
- A Gray Hole might exhibit its mischievous behavior in several techniques.
- It simply drops packets coming from (or intended to) positive exact node(s) in the grid while advancing all the packets for other nodes.
- Another type of Gray Hole attack is a knot performs innocently for some specific time duration by dropping packets but may switch to normal behavior earlier.
- A Gray Hole might also exhibition a behavior which is a mixture of the above two, thereby making its detection even more difficulty**.**[12]

VII. ROUTING PROTOCOL IN MANET

Classification of routing protocols in MANET's can be done in many ways, but most of these are complete contingent on routing plan and network construction. According to the routing strategy the routing procedures can be branded as Table-driven and basis initiated, while contingent on the network structure these are secret as flat direction-finding, hierarchical direction-finding and geographic location assisted routing. Both the Table-driven & basis started protocols originate under the Smooth routing

A. Table-Driven routing protocols (Proactive): These protocols are likewise named as proactive protocols meanwhile they maintain the routing information even before it is needed. All and every knob in the network maintains routing information to every other node in the network. Routes data is usually kept in the routing counters and is occasionally updated as the grid topology changes. Many of these routing procedures come since the link-state direction-finding [8]. There exist some differences between the protocols that come under this class contingent on the routing data being efficient in each routing counter.

B. On Demand routing protocols (Reactive): These rules are also named reactive rules since they don't maintain routing information or routing activity at the scheme knobs if now is no communication. If a knob wants to send a packet to another node then this protocol explorations for the way in an on- demand scheme and originates the connection in order to transmit and receive the packet. The direction discovery typically occurs by drowning the route request packets throughout the network**.**

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 9, ISSN No. 2455-2143, Pages 83-89
Published Online July – August 2016 in IJEAST (http://www.ijeast.com)

VIII. DIFFERENCE AMONG REACTIVE, PROACTIVE AND CROSSBREED ROUTING PROTOCOLS.

Proactive	**Reactive**	**Crossbreed**
• Proactive routing protocols remain also named as table ambitious routing protocols. • In this every node maintain routing table which contains data around the network structure even devoid of needful it. • This feature although useful for datagram traffic, incurs considerable gesturing traffic and energy consumption. • The routing tables are updated periodically when the grid topology variations. Proactive procedures are not appropriate for large networks as they need to maintain node records for every single and every other knob in the routing table of all nodes. • These protocols maintain different number of routing table's variable from rules to rule. There are various well known proactive routing protocols. • Example: DSDV, OLSR, WRP etc.	• Reactive routing protocol is also known as on demand routing protocol. • In this protocol route is discovered every time it is wanted Nodes recruit route detection on demand basis. • Source node sees its route cache for the obtainable route since source to endpoint if the direction is not available then it initiates route discovery process. • The on- request direction-finding rules have two main mechanisms	• There is a trade-off between proactive and reactive protocols. Proactive rules have great above and less dormancy while reactive rules have less overhead and more latency. • So a Cross procedure is obtainable to overwhelmed the shortcomings of both proactive and reactive routing protocols. • Hybrid direction-finding procedure is combination of both active and reactive routing protocol. Hybrid protocol is suitable for large grids where huge amounts of nodes are exists. In this large network is divided into set of zones where routing confidential the zone is achieved by using reactive method and outside the zone routing is done using reactive approach. • Here are several popular hybrid direction-finding rules for MANET like ZRP, SHARP.

IX. CONCLUSION

A great development in the area of wire-less systems (substructure created) and in the field of Mobile ad hoc network (substructure less system). Here amount of routing procedures for MANET, where broadly categorized as proactive and sensitive and Crossbreed rules. Black-hole & Gray-hole remain one of the serious threats in mobile ad hoc network. It affects the performance of the different routing protocol such as AODV by injecting a false route answer message and it similarly growths the network traffic.

X. REFERENCES

[1] P. Huang, L. Xiao, S. Soltani, M. W. Mutka, and N. Xi, "The Evolution of MAC Protocols in Wireless Sensor Networks: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 1, pp. 101–120, 2013.

[2] D. Bhattacharyya, T. Kim, and S. Pal, "A Comparative Study of Wireless Sensor Networks and Their Routing Protocols," *Sensors*, vol. 10, no. 12, pp. 10506–10523, 2010.

[3] K. Maraiya, K. Kant, and N. Gupta, "Application based Study on Wireless Sensor Network," *Int. J. Comput. Appl.*, vol. 21, no. 8, pp. 9–15, 2011.

[4] J. Anju and C. N. Sminesh, "An Improved Clustering-Based Approach for Wormhole Attack Detection in MANET," *Proc. - 2014 3rd Int. Conf. Eco-Friendly Comput. Commun. Syst. ICECCS 2014*, pp. 149–154, 2015.

[5] M. Alikhany and M. Abadi, "A dynamic clustering-based approach for anomaly detection in AODV-based MANETs," *2011 Int. Symp. Comput. Networks Distrib. Syst. CNDS 2011*, pp. 67–72, 2011.

[6] D. B. Roy and R. Chaki, "MCBHIDS: Modified layered cluster based algorithm for black hole IDS," *2013 Annu. IEEE India Conf. INDICON 2013*, 2013.

[7] J. Savner and V. Gupta, "Clustering of mobile ad hoc networks: An approach for black hole prevention," *2014 Int. Conf. Issues Challenges Intell. Comput. Tech.*, pp. 361–365, 2014.

[8] Z. Hussain, M. P. Singh, and R. K. Singh, "Analysis of Lifetime of Wireless Sensor Network," vol. 53, pp. 117–126, 2013.

[9] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey," *Secur. Distrib. Grid, Mobile, Pervasive Comput.*, pp. 367–410, 2007.

[10] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," *IEEE Wirel. Commun.*, vol. 14, no. 5, pp. 85–91, 2007.

[11] M. Tripathi, M. S. Gaur, and V. Laxmi, "Comparing the impact of black hole and gray hole attack on LEACH in WSN," *Procedia Comput. Sci.*, vol. 19, pp. 1101–1107, 2013.

[12] K. Gorantala, "Routing protocols in mobile ad-hoc networks," *Master's Thesis Comput. Sci. June*, 2006.