IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-3, Issue-5 E-ISSN: 2347-2693

Survey of Attacks and Security Schemes in Wireless Sensor Network

Sonam Jai*, Deepak Singh Tomar and Rachana Kamble

Department of computer science & Engineering, TIT, Bhopal

www.ijcseonline.org

Received: April/25/2015 Revised: May/02/2015 Accepted: May/9/2015 Published: May/30/2015

***Abstract*—** Wireless Sensor Networks are emerging as the latest tier for data monitoring in many applications like commercial, industrial, military etc. Security in WSN's is one of the major challenges in order to provide protected and authenticated communication between sensor nodes. However providing secure routing in WSN is a matter of fundamental concern. Although a wide variety of routing protocols have been proposed for WSN's but most of them do not take security into account as a main goal. Routing attacks can have devastating effects on WSNs .Hence it is the major challenge when designing robust security mechanism for WSNs. In this paper ,we examine some of the most common routing attacks, routing protocols and security schemes in WSNs. It is suggested that in order to overcome the challenges of routing attacks in WSNs , some new routing protocols or strategy must be carefully designed so that attacks can be rendered meaningless .

Keywords— WSN, Security, Attack, Routing. Survey

I. INTRODUCTION

Wireless Sensor Networks (WSNs) consist of spatially distributed autonomous small devices that cooperatively monitor environmental or physical conditions in remote and often hostile environments. Due to recent advancement in technology, the manufacturing of small and low cost sensors have become technically and economically feasible. The sensing devices measures the ambient condition related to the environment which surrounds them and transforms them into an electric signal. Processing such a signal reveals some properties about objects located or events happening in the vicinity of the sensor. Such type of sensors can be networked in many applications that require unattended operations. A Wireless Sensor Network (WSN) contains hundreds or thousands of these sensor nodes. These sensors have the ability to communicate either among each other or directly to an external base-station (BS). A greater number of sensors allows sensing over larger geographical regions with greater accuracy. Wireless Sensor Networks (WSN) [1] consists of numerous tiny sensors deployed at high density in regions requiring surveillance and monitoring. The sensors are deployed at a cost much lower than the traditional wired sensor system. The deployement of large number of sensors enables to have more accurate measurements. A Sensor Node consists of one or more sensing elements (motion, temperature, pressure, etc.), a battery, low power radio trans-receiver, microprocessor, limited memory, mobilizer (optional),and a position finding system[2]. An important aspect of such networks is that, the nodes are unattended, have limited energy and the network topology is unknown. Many design challenges that arise in sensor networks are because of limited resources they have and their deployment in hostile environments. A Wireless Sensor Network (WSN) is a particular type of ad-hoc network. The nodes exchange data in order to build a global view of the monitored region Figure 1. This data is typically made accessible to the user through one or more gateway nodes [3].

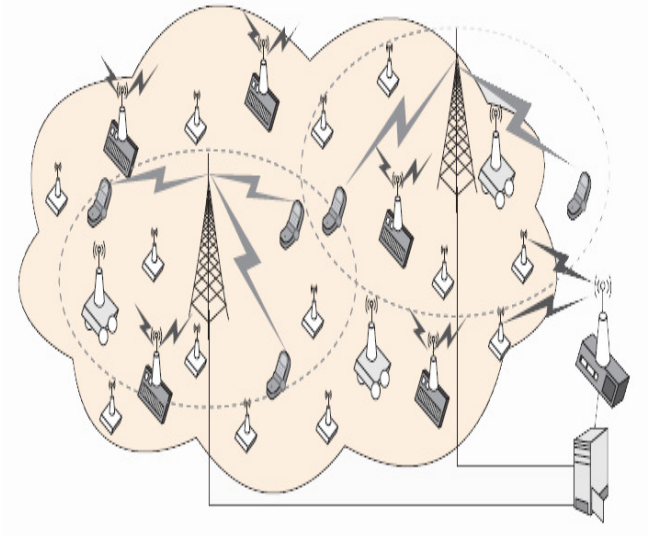


Figure 1 Example of WSN

Fig. 1 shows the schematic diagram of sensor node components. Basically, each sensor node comprises sensing, processing, transmission, mobilizer, position finding system, and power units (some of these components are optional like the mobilizer). The same figure shows the communication architecture of a WSN. Sensor nodes are usually scattered in a sensor field, which is an area where the sensor nodes are deployed. Sensor nodes coordinate among themselves to produce high-quality information about the physical environment.

II. CHARACTERISTICS OF WSN

The characteristics of sensor network have a decisive impact on the network design objectives in term of network capabilities and network performance .

© 2015, IJCSE All Rights Reserved

Wireless sensor networks have the following unique characteristics and constraints when compared to traditional wireless communication networks like cellular network and mobile adhoc network(MANET) :

Dense sensor node deployment: Sensor nodes are usually densely deployed and can have several orders of magnitude higher than that in a MANET.
Battery-powered sensor nodes: Sensor nodes are usually powered by battery and are deployed in a harsh environment where it is very difficult to alter or recharge the batteries.
Severe energy, computation, and storage constraints: Sensors nodes are having highly limited energy, computation, and storage capabilities.
Self-configurable: Sensor nodes are usually randomly deployed and autonomously configure themselves into a communication network.
Unreliable sensor nodes: Since sensor nodes are prone to physical damages or failures due to its deployment in harsh or hostile environment.
Data redundancy: As the sensor nodes are densely deployed in a region of interest and they collaborate to accomplish a common sensing task. Thus, the data sensed by multiple sensor nodes typically have a certain level of correlation or redundancy.
Application specific: A sensor network is usually designed and deployed for a specific application. The design requirements of a sensor network change with its application.
Many-to-one traffic pattern: In most sensor network applications, the data sensed by sensor nodes flow from multiple source sensor nodes to a particular sink, exhibiting a many-to-one traffic pattern.
Frequent topology change: Network topology changes frequently due to the node failures, damage, addition, energy depletion, or channel fading.

III. WSN DESIGN OBJECTIVES

As the Sensor networks are application specific, the following main design objectives are kept under consideration in the design of sensor networks:

Small node size: The reduction in node size can facilitate dense node deployment in hostile and harsh environment. It will also reduce the power consumption and cost of sensor nodes.

Low node cost: Since sensor nodes are usually densely deployed in a ruthless environment and cannot be reused, hence reducing the cost of sensor nodes is important which in turn will result into the cost reduction of whole network.

Low power consumption: It is crucial to reduce the power consumption of sensor nodes so that the lifetime of the sensor nodes, as well as the whole network is prolonged.

Scalability: Since the number sensor nodes in sensor networks are in the order of tens, hundreds, or thousands, network protocols designed for sensor networks should be scalable to different network sizes.

Reliability: Network protocols designed for sensor networks must provide error control and correction mechanisms to ensure reliable data delivery over noisy, error-prone, and time-varying wireless channels.

Self-configurability: In sensor networks, once deployed, sensor nodes should be able to autonomously organize themselves into a communication network and reconfigure their connectivity in the event of topology changes and node failures.

Adaptability: In sensor networks, a node may fail, join, or move, which would result in changes in node density and network topology. Thus, network protocols designed for sensor networks should be adaptive to such density and topology changes.

Channel utilization: Since sensor networks have limited bandwidth resources, communication protocols designed for sensor networks should efficiently make use of the bandwidth to improve channel utilization.

Fault tolerance: Sensor nodes are prone to failures due to harsh deployment environments and unattended operations. Thus, sensor nodes should be fault tolerant and have the abilities of self testing, self-calibrating, self-repairing, and self-recovering.

Security: A sensor network should introduce effective security mechanisms to prevent the data information in the network or a sensor node from unauthorized access or malicious attacks.

QoS support: In sensor networks, different applications may have different quality-of-service (QoS) requirements in terms of delivery latency and packet loss. Thus, network protocol design should consider the QoS requirements of specific applications.

IV. ROUTING PROTOCOLS IN WSN

Routing in wireless sensor networks differs from conventional routing in fixed networks in various ways. There is no infrastructure, wireless links are unreliable, sensor nodes may fail, and routing protocols have to meet strict resources requirements [4][5][6]. Routing paths can be established in one of three ways, namely proactive, reactive or hybrid.. According to how the information is acquired, the routing protocols can be classified into proactive, reactive and hybrid routing.

A. Proactive (table-driven) Routing Protocol

Proactive protocols compute all the routes before they are really needed and then store these routes in a routing table in each node. When a route changes, the change has to be propagated throughout the network. Since a WSN could consist of thousands of nodes, the routing table that each

© 2015, IJCSE All Rights Reserved

node would have to keep could be huge and therefore proactive protocols are not suited to WSNs.The proactive routing Protocol is also known as table-driven routing protocol. In this routing protocol, mobile nodes periodically broadcast their routing information to the neighbour's nodes. Each node needs to maintain their routing table of not only adjacent nodes and reachable nodes but also the number of hops. Therefore, the disadvantage is the rise of overhead due to increase in network size, a significant big communication overhead within a larger network topology. However, the major advantage is of knowing the network status immediately if any malicious attacker joins. The most familiar types of the proactive routing protocol are: - *Destination sequenced distance vector (DSDV) routing protocol*

B. Reactive (on-demand) Routing Protocol

The reactive routing protocol is equipped with another appellation named on-demand routing protocol. In compare to the proactive routing, the reactive routing is simply starts when nodes desire to transmit data packets. The major advantage is the reduction of the wasted bandwidth induced from the cyclically broadcast. The disadvantage of reactive routing protocol method is loss of some packet. Here we briefly describe two prevalent on-demand routing protocols which are: Ad hoc on-demand distance vector (AODV) and Dynamic source routing (DSR) protocol.

C. Hybrid Routing Protocol

The hybrid routing protocol as the name suggests have the combine advantages of proactive routing and reactive routing to overcome the defects generated from both the protocol when used separately. Design of hybrid routing protocols are mostly as hierarchical or layered network framework. In this system initially, proactive routing is employed to collect unfamiliar routing information, and then at later stage reactive routing is used to maintain the routing information when network topology changes. The familiar hybrid routing protocols are: - Zone routing protocol (ZRP) [7].

V. WSN CHALLENGES AND ROUTING ISSUES

The design of routing protocols for WSNs is challenging because of several network constraints. WSNs suffer from the limitations of several network resources, for example, energy, bandwidth, central processing unit, and storage [8][9]. The design challenges in sensor networks involve the following main aspects [3][8][9]:

Limited energy capacity: Since sensor nodes are battery powered, they have limited energy capacity. Energy poses a big challenge for network designers in hostile environments, for example, a battlefield, where it is impossible to access the sensors and recharge their batteries. Furthermore, when the energy of a sensor reaches a certain threshold, the sensor will become faulty and will not be able to function properly, which will have a major impact on the network performance. Thus, routing protocols designed for sensors should be as energy efficient as possible to extend their lifetime, and hence prolong the network lifetime while guaranteeing good performance overall.

Sensor locations: Another challenge that faces the design of routing protocols is to manage the locations of the sensors. Most of the proposed protocols assume that the sensors either are equipped with global positioning system (GPS) receivers or use some localization technique [7] to learn about their locations.

Limited hardware resources: In addition to limited energy capacity, sensor nodes have also limited processing and storage capacities, and thus can only perform limited computational functionalities. These hardware constraints present many challenges in software development and network protocol design for sensor networks, which must consider not only the energy constraint in sensor nodes, but also the processing and storage capacities of sensor nodes.

Massive and random node deployment: Sensor node deployment in WSNs is application dependent and can be either manual or random which finally affects the performance of the routing protocol. In most applications, sensor nodes can be scattered randomly in an intended area or dropped massively over an inaccessible or hostile region. If the resultant distribution of nodes is not uniform, optimal clustering becomes necessary to allow connectivity and enable energy efficient network operation.

Network characteristics and unreliable environment: A sensor network usually operates in a dynamic and unreliable environment. The topology of a network, which is defined by the sensors and the communication links between the sensors, changes frequently due to sensor addition, deletion, node failures, damages, or energy depletion. Also, the sensor nodes are linked by a wireless medium, which is noisy, error prone, and time varying. Therefore, routing paths should consider network topology dynamics due to limited energy and sensor mobility as well as increasing the size of the network to maintain specific application requirements in terms of coverage and connectivity.

Data Aggregation: Since sensor nodes may generate significant redundant data, similar packets from multiple nodes can be aggregated so that the number of transmissions is reduced. Data aggregation technique has been used to achieve energy efficiency and data transfer optimization

in a number of routing protocols.

Diverse sensing application requirements: Sensor networks have a wide range of diverse applications. No network protocol can meet the requirements of all applications. Therefore, the routing protocols should guarantee data delivery and its accuracy so that the sink can gather the required knowledge about the physical phenomenon on time.

Scalability: Routing protocols should be able to scale with the network size. Also, sensors may not necessarily have the same capabilities in terms of energy, processing,

© 2015, IJCSE All Rights Reserved

sensing, and particularly communication. Hence, communication links between sensors may not be symmetric, that is, a pair of sensors may not be able to have communication in both directions. This should be taken care of in the routing protocols.

VI. SECURITY THREATS IN WSN

It defines the intrusion as any set of actions that are attempting to compromise the main components of the security system

1) The integrity,

2) Confidentiality or availability of a resource.

In the same work, the intruder therefore was defined as an individual or group of individuals who take the action in the intrusion. The plainness of many routing protocols for wireless sensor networks makes them an easy target for the attacks. T are classifies the routing attacks into the following categories;

1) Spoofed, Altered, or Replayed Routing Information

While sending the data, the information in transition may be spoofed, altered, replayed, or destroyed. Due to the short range transmission of the sensor nodes, an attacker with high processing power and larger communication range could attack several sensors simultaneously and modify the transmitted information.

2) Selective Forwarding

In this kind of attack a malicious node may decline to forward every message it gets, acting

as black hole or it can forward some messages to the wrong receiver and simply drop others.

3) Sinkhole Attacks

In the Sinkhole attack, the goal of the attacker is to attract all the traffic. Especially, in the case of a flooding based protocol the compromised node may listen to requests for routes, and then reply

to the requesting node with messages containing a bogus route with the shortest path to the requested destination.

4) Sybil Attacks

In Sybil attack the malicious node presents itself as multiple nodes. The attack of this type tries to degrade the usage and the efficiency of the distributed algorithms that are used. Sybil attack can be performed against distributed storage, routing, data aggregation, voting, fair resource allocation, and misbehavior detection [7].

5)Wormholes Attack: Wormhole attack [12] is an attack in which the malicious node tunnels messages from one part of the network over a link, that doesn't exist normally, to another part of the network. For example Fig 2 shows the WSN when there is no attack in the network . The data transmits through the best path chosen for it as here source A transmits data to destination E via B,C,D.

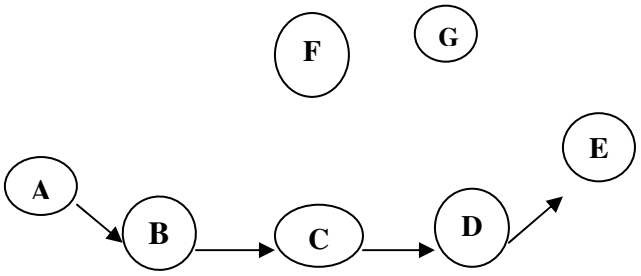
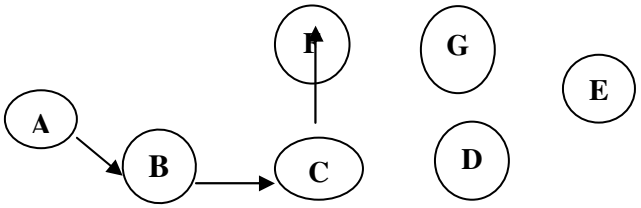


Figure 2 WSN when there is no attack.

Now say C is a node who is intruder in our network and instead of forwarding the packets to D it starts relaying the packets to its friend neighbor F who keeps on dropping or capturing the data packets ,hence packets cannot reach the destination node i.e. node E .This tunneling between malicious node C and F is termed as Wormhole attack as shown below in figure 3 .



6)

Figure 3 Worm Hole attack betweent node C and F.

7) HELLOFloodAttacks

This attack is based on the use by many protocols of broadcasting Hello messages to announce themselves in the network. So an attacker with higher range of transmission may send many Hello messages to a large number of nodes in a big area of the network. These nodes are then convinced that the attacker is their neighbor. Consequently the network is left in a state of confusion.

8) Acknowledgement

Some wireless sensor network routing algorithms require link layer acknowledgements. A compromised node may exploit this by spoofing these acknowledgements, thus convincing the sender that a weak link is strong or a dead sensor is alive.

9) Sleep deprivation attack

A particularly devastating attack is the sleep deprivation attack, where a malicious node forces legitimate nodes to waste their energy by resisting the sensor nodes from going into low power sleep mode. The goal of this attack is to maximize the power consumption of the target node, thereby

© 2015, IJCSE All Rights Reserved

decreasing its battery life. So, it is also known as battery exhaustion attack.

VII. SECURITY SCHEMES IN WSN

Security schemes are providing the free environment from malicious nodes. Security defines the mechanism to handle undesired operations in specifically generated conditions to degrade the network performance. These planned conditions are known as attacks. Due to the dynamic nature of MANET, it is affected most by the attackers. There are so many attacks like, black-hole, wormhole, flooding, packet drops, masquerade etc which creates misbehaving nodes in the network whose aim is to let the network actual functioning down. Security is mainly involved with military applications using sensor networks in critical conditions. Thus a network is taken as a secure if it holds following properties for transmissions [3]:

Sno	Property	Description
1	Availability	Ensures that the network manages to provide all services despite when denial of service attacks occurred intentionally.
2	Confidentiality	Ensures that certain information is never disclosed to unauthorized users in any routing scenario.
3	Integrity	Guarantees that the message that is transmitted reaches its destination without being changed or corrupted in any way.
4	Authentication	Enables a node to be sure of the identity of the peer with which it communicates
5	Non-Repudiation	Ensures that the originator of a message cannot refuse sending this message.

In this paper [12] an improved watchdog monitoring mechanism is proposed by using the process of change point detection. By implementing this change point detection algorithm in watchdog mechanism, the limitations of the existing watchdog mechanism are overcome. From this the exact malicious node can be found out and the data will be routed through a secure path bypassing the malicious node. Finally to analyze the efficiency of this algorithm, the results obtained from the proposed algorithm and the existing algorithms are compared.

In this paper [13] has a tendency to opt for Bio-Inspired Approach. In this paper, the clonal selection principle is implemented and develop the Watchdog based Clonal Selection Algorithm (WCSA).Using this WCSA, the intrusions in the network and monitoring multiple misbehaved nodes. Using this algorithm we can realize intruders and reduce the detector rate, and reduce generator value also will increase in throughput.

In [14] Rule-based intrusion detection schemes is proposed for WSN, also called specification based intrusion detection schemes. In these schemes, the detection rules are first designed by domain expert before the starting the detection process. Most of the techniques in these schemes follow three main phases: data acquisition phase, rule application phase and intrusion detection phase. In the following sub-sections, the key important schemes in this category are explored.

Decentralized IDS in WSN propose the first and the most cited rule-based intrusion detection scheme for WSN to detect many different kinds of attacks in different layers. In this scheme, there are three main phases involved: data acquisition phase in which the monitor nodes are responsible of promiscuous listening of the messages and filtering the important information for the analysis; the rule application phase, in which the pre-defined rules are applied to the stored data from the previous phase, if the message analysis failed any of the rules test, a failure is raised and the counter increased by one; the intrusion detection phase, a comparison is taken place between the number of raised failures produced from the rule application phase with a predefined number of occasional failures that may happen in the network. If the total number of the raised failures is higher, intrusion alarm is produced.

According to [15] this scheme brings a good framework to the class of rule-based intrusion detection. But, there is an important drawback of this scheme, which is the ambiguity in determining the number of monitoring nodes dedicated to the detection process, the way of choosing them and how to make sure that the way of selection will cover the entire network. In addition, this scheme is restricted to some types of attacks and the question which may rise up is what if new types of attacks emerge? All these drawbacks should be considered when designing any kind of intrusion detection scheme.

In [16] Malicious node detection in WSN presents a solution to identify the possible malicious node based on the received signal strength measured in each node. They showed how to detect two kinds of attacks called HELLO flood attack and the wormhole attack in WSN by building a rule that compare the energy of the received signal and the energy of the same observed signal around the network. Although, this solution was one of the first solutions in the domain, it still restricted to those two types of attacks. In

© 2015, IJCSE All Rights Reserved

addition, sometimes there are other reasons rather than attacks that may cause a change in the signal strength which make this solution impractical.

A novel intrusion detection scheme [17] that takes the benefits of neighboring node information to detect the node impersonation and resource depletion attacks has been proposed. In this scheme each node can make a statistical profile of its neighbor's behavior based on two features which are the received power rate and the arrival packet rate. This scheme cannot to be generalized for a typical wireless sensor network application in which many types of attacks evolve continuously. In addition and similar to the scheme proposed in [20], the building of the rules based on the received power rate is impractical since there are other factors that may affect this feature.

Towards intrusion detection in [18] introduce a lightweight scheme for detecting selective forwarding and black hole attacks in WSN. The key idea of their scheme is to make nodes monitor their neighborhood and then communicate between each other to decide if there is an intrusion taken place. The scheme is further evaluated experimentally on a real WSN deployment. This scheme benefits from the neighbors monitoring so that there is a kind of distribution that will minimize the computation load on a detection agent node. However, there will be an increase in the communication messages between nodes during the collaboration for voting that will increase the communication overhead and as a result will deplete the power of nodes quickly. It is clear that, this scheme lacks the generality that other schemes in the same category.

Intrusion detection scheme of sinkhole attack in WSN is a more specific intrusion detection scheme to detect sinkhole attack was proposed by [19]. This scheme is composed of four modules: Local Packet Monitoring Module, Local Detection Engine Module, Cooperative Detection Engine and Local Response Model. The proposed scheme has been implemented in the Tiny OS environment with Min Route protocol. A suitable detection rules have been prepared to suite with the sinkhole attack. Generally, this scheme satisfies the distribution feature of IDS which is highly required on a large scale and autonomous environment like WSN. The problem here still with the communication overhead between the nodes to exchange useful information that helps in detecting the attack.

In [20] present an intrusion detection architecture based on collaboration between neighbors. They evaluated their scheme for detecting three types of attacks: Hello flood, selective forwarding and jamming attacks. Their scheme was implemented for Collaboration Tree Protocol (CTP) on the Tiny OS environment. Although, the collaboration among nodes makes this scheme strong, the communication overhead is a problem. In addition, the extracted features that are used to construct the rules like packet sending rate and packet dropping rate caused a high false alarm for detecting attacks. Another drawback of this study is that it did not consider the power consumption rate related to the performance which is a very critical issue in WSNs.

A collaborative IDS scheme has been proposed in [21], to detect node repetition attacks. This scheme is based on determining some nodes to be monitored nodes for monitoring the behavior of other nodes in the network based on satisfying set of predefined rules suitable for a specific attack type. These monitor nodes are in turn monitored by special nodes called supervisor nodes which are responsible for correlating the evidences resulted by monitor nodes. Although, this scheme seems robust in protecting the network by using two layers of protection, there are some drawbacks that limit the usefulness of this scheme. To begin with, the supervisor nodes could be sources of failure if they have been compromised. Another drawback is related to the generality which is a major problem for the most rule-based schemes for intrusion detection. Many assumptions have been made for designing this scheme which caused inflexibility of application.

VIII. CONCLUSION

Secure routing is crucial to the acceptance and use of sensor networks for many applications. Providing secure routing in WSNs is a complicated and challenging task due to the inherently constrained capabilities of sensor nodes.A variety of countermeasures have been proposed in the literature for attacks.

Routing attacks can have potentially devastating effects on WSNs and present a major challenge when designing robust security mechanisms for WSN. Although many different routing protocols have been proposed for WSN, most do not take security into account as a main goal. We briefly looked at some of the most common routing attacks in WSN. In particular, we looked at the wormhole attack in some detail. Although a number of different countermeasures have been proposed for this attack, most of these suffer from flaws that essentially render them ineffective for large scale WSN deployments.

IX. REFERENCES

[1] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks", Attacks and Countermeasures", Ad Hoc Networks (elsevier), Page: 299-302, 2003.

[2] Santi, P. "Topology control in wireless ad hoc and sensor networks" Chichester, England: John Wiley & Sons, 2005.

[3] Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEE, 2009.

[4] Clement Ogugua Asogwa, Xiaoming Zhang, Degui Xiao, Ahmed Hamed, "Experimental Analysis of AODV, DSR and DSDV Protocols Based on Wireless Body Area Network" Communications in Computer

© 2015, IJCSE All Rights Reserved

and Information Science,Springer-VerlagBerlin Heidelberg,Volume 312, pp 183-191, 2012.

[5] Faleh Rabeb, Nasri Nejah, Kachouri Abdennaceur,Samet Mounir, "An Extensive Comparison among DSDV, DSR and AODV Protocols in wireless sensor network" IEEE, International Conference on Education and e-Learning Innovations, 2012.

[1] Nasrin Hakim Mithila, "Performance analysis of DSDV, AODV and DSR in Wireless Sensor Network" International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE) Volume 2, Issue 4, pp.395-404, April 2013

[2] Ipsita Panda "A Survey on Routing Protocols of MANETs by Using QoS Metrics" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, pp. 121-129, 2012.

[6] Jamal Al-Karaki, and Ahmed E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey", IEEE Communications Magazine, vol 11, no. 6, pp. 6-28, Dec. 2004.

[7] 13. Kemal Akkaya and Mohamed Younis, "A Survey on Routing Protocols for Wireless Sensor Networks", Ad hoc Networks, vol. 3, no. 3, pp. 325-349, May 2005.

[8] 5.C. Karlof and D. Wagner, Secure Routing in Sensor Networks: Attacks and Countermeasures, In Proc. of First IEEE International Workshop on Sensor Network Protocols and Applications, 2003.

[9] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less Low Cost Outdoor Localization for Very Small Devices", IEEE Personal Communication Magazine, vol. 7, no. 5, pp. 28-34, Oct. 2000

[10] A.Babu Karuppiah, T.Meenakshi, T.I.Mano Ranjitha & S.Vivitha, " False Misbehaviour Elimination in Watchdog Monitoring System Using Change Point in a Wireless Sensor Network", An International Journal on Graduate Research in Engineering and Technology (GRET), pp. 31-35, 2013

[11] S. Nishanthi, "Intrusion Detection in Wireless Sensor Networks Using Watchdog Based Clonal Selection Algorithm", IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013

[12] Silva, A.P.R.D., M.H.T. Martins, B.P.S. Rocha, A.A.F.Loureiro and L.B. Ruiz, "Decentralized Intrusion Detection In Wireless Sensor Networks" Proceedings of the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks, (QSSWMN; 25), pp: 16-23, 2005

[13] Xie, M., S. Han, B. Tian and S. Parvin, "Anomaly detection in wireless sensor networks: A survey" Journal of Network and Computer Application, pp.1302-1325, 2011

[14] Pires, W.R., T.H. De Paula Figueiredo, H.C. Wong and A.A.F. Loureiro, "Malicious node detection in wireless sensor networks", Proceedings. 18th International, Parallel and Distributed Processing Symposium, (PDS' 04), pp: 1-7, 2004.

[15] Onat, I. and A. Miri, "An Intrusion Detection System For Wireless Sensor Networks", Proceedings of the IEEE International Conference on, Wireless And Mobile Computing, Networking And Communications, IEEE Xplore Press, pp: 253-259, Aug. 22-24, 2005.

[16] Krontiris, I., T. Dimitriou and F.C. Freiling, "Towards Intrusion Detection In Wireless Sensor Networks", Proceeding of the 13th European Wireless Conference, CiteSeer, 2007.

[17] Krontiris, I., T. Dimitriou, T. Giannetsos and M. Mpasoukos, "Intrusion Detection Of Sinkhole Attacks In Wireless Sensor Networks" Proceedings of the 3rd International Conference on Algorithmic Aspects of Wireless Sensor Networks, (AAWSN' 28), Springer-Verlag Berlin, Heidelberg, pp: 150- 161, 2008.

[18] Stetsko, A., L. Folkman and V. Matyáš, "Neighbor-Based Intrusion Detection For Wireless Sensor Networks". Proceedings of the 6th International Conference on Wireless and Mobile Communications (ICWMC), IEEE Xplore Press, Valencia, pp: 420-425, Sept. 20-25, 2010.

[19] Lemos, M.V.D.S., L.B. Leal and R.H. Filho, "A New Collaborative Approach for Intrusion Detection System on Wireless Sensor Networks", Novel Algorithms Techniques Telecommunication Network, pp. 239-244, 2010.

[20] Shio Kumar Singh, M P Singh, and D K Singh"A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks" International Journal of Computer Trends and Technology (IJCTT) pp. 1-9, May to June 2011.

© 2015, IJCSE All Rights Reserved