ASIAN JOURNAL OF INFORMATION TECHNOLOGY

MEDWELL PUBLICATIONS

Wireless Sensor Networks: A Survey on Recent Developments in Sensors Security

A. Kathirvel and M. Subramaniam
Department of Computer Science and Engineering, SRM Institute of Science and Technology, Vadapalani Campus, Chennai, India

Key words: WSN, routing, security, protocols, future, technologies

Corresponding Author:
A. Kathirvel
Department of Computer Science and Engineering, SRM Institute of Science and Technology, Vadapalani Campus, Chennai, India

Page No.: 1-13
Volume: 20, Issue 1, 2021
ISSN: 1682-3915
Asian Journal of Information Technology

Abstract: Wireless Sensor Network (WSN) has arisen as one of the most encouraging technologies for the future computing system. It has been enabled by advances in today's recent technology and it is available in very small, low expensive and intelligent smart sensors resulting in cost effective and easily deplorable WSNs in anywhere else. Conversely, academics and scientist must number of challenges to facilitate the widespread deployment of Wireless sensor network technology in real-world situation. In this study, we have made survey on recent developments in sensors security, we give a synopsis of wireless sensor networks and their application domains including the security challenges that should be addressed in order to push the technology further. Finally, we have identified several open research issues not addressed so for that need to be investigated in future. Our work is totally different from existing work in that, we focus on recent developments in wireless sensor network technologies. We review the leading research projects, standards and technologies and platforms. This study, very helpful to the new academics and scientist, researchers entering the domain of wireless sensor network by providing a comprehensive work on recent developments in security issues.

INTRODUCTION

Fundamentals of WSN and motivation

Wireless sensor networks: A rapid advancement in recent digital information technology has made it possible to transmit the data in wireless links without the aid of any fixed infrastructure. Wireless Sensor Network (WSN) is a group of sensors, plugged for some dedicated application to monitoring and recording the physical conditions of the natural environment. IEEE 802.15.4 WSN is organizing the collected data at a centralized server in the secured location. It will measure environmental conditions like Earth climatic temperature, environmental noise and environmental pollution levels, sound, humidity, wind and enemy crossing in the country border, etc. Thus, a set of wireless sensor nodes are used to dynamically exchange data among themselves even in the presence of a predetermined infrastructure and centralized controller. Some nodes also act as a router allowing other users to communicate through their receiving communication devices as shown in Fig. 1.

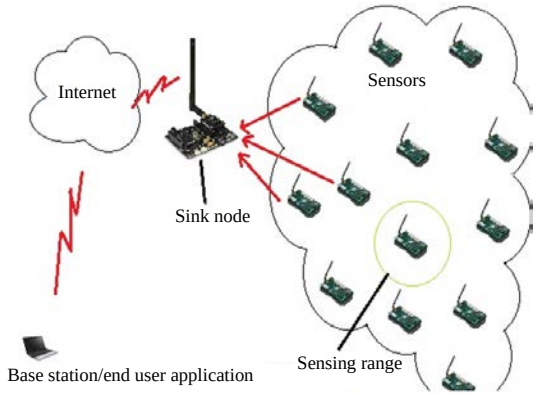

Fig. 1: Wireless sensor networks

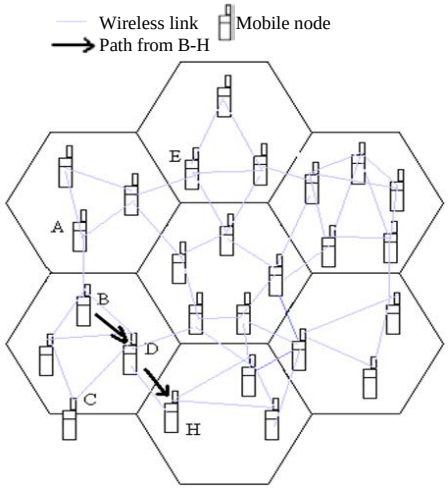

Fig. 2: A Mobile ad hoc wireless network

The transmitting communication range of each sensor device is very limited, therefore, at any given time a user can exchange data and control packets only with any one of the devices in its sensor transmitting or sensor receiving range. In wireless sensor network, nodes may drain their battery power (i.e.,) nodes are not in position to communicate, thus new route are used to transmit the data through new network topology, causing frequent link disconnection in the network. Moreover, the network bandwidth of any wireless communication channel is limited. Wireless sensor nodes in the networks operate on resource constrained battery energy power which gets fatigued within a time span sooner or later depending on network usage. Wireless sensor network is subset of Mobile Ad Hoc Networks (MANETs). In MANET, the path setup for a mobile node call between two nodes, say, the node B to the node H is illustrated in Fig. 2.

Difference between Wireless Sensor Networks (WSN) and MANETs is given below. Usually WSN

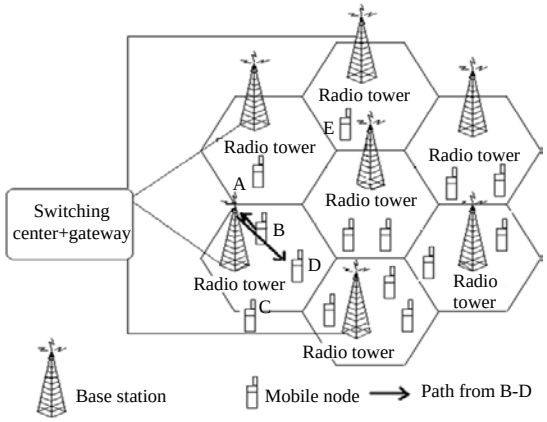

Fig. 3: A cellular network

consists of one sink (or base station) able to manage all the communications between other nodes. This network has fixed routes, excepting when there are node's failures. Thus, the base station determines and optimizes the paths of communication in the network.

A Mobile Ad-hoc Network (MANET) even is a WSN if its scope is that of sensing the environment around the network. However, the words "mobile" and "ad-hoc" are often used to refer to all those networks consisting of nodes continuously moving in any direction illustrated in Fig. 2. Consequently, this kind of network must repeatedly reconfigure its routes. All this work is done by every node in the network since MANET doesn't have a fixed central controller (i.e., ad hoc). Examples of MANETs are networks formed by devices installed within cars (VANET) to monitor accidents, traffic and so on or a network consisting of drones.

Unlike the conventional cellular networks (depicted in Fig. 3) that rely on widespread infrastructure to support node mobility, a wireless MANET does not need costly network base stations and wired network infrastructure. These features are very important for possible to use in a wide mixture of dissimilar situations. Such dissimilar situations include war battlefield communications and throwaway sensors which are sensors dropped from high altitudes and are isolated on the ground station for the detection of very hazardous materials.

Civilian people applications include disaster situations such as quick responses to earth hurricane, ocean tsunami, land and ocean earthquake and terrorist attacks. Another remarkable example is the case where a set of mobile vehicles such as car, bus, truck, motor cycle etc, on the highway form an mobile ad hoc network of their own in order to give vehicular traffic management system called VANET. Security concern in the wireless mobile ad hoc networks plays a vital part in shaping the success of network people centric warfare as envisioned

for future secure military operations. Thus, network security is a main issue for these assignment dangerous applications. All these limits and constraints make wireless MANET research trickier.

CHALLENGES IN ROUTING PROTOCOLS FOR WSN

Routes in wireless sensor networks are multi-hop wireless sensor radio relaying because of the limited radio propagation range (200 m) of wireless radios. Wireless sensors nodes are remain at position still. Sensor nodes may fail at any time due to battery drain or chip failures etc and network routes may frequently get disconnected. Network routing protocols are answerable for network maintaining and new route reconstructing the routes in a appropriate manner as well as establishing the robust routes. In addition, network routing protocols are required to execute all the above tasks lacking generating too much control message overhead. Routing control message packets must be utilized well to deliver packets and be generated only when needed. To reducing the control packets can construct the routing protocol efficient by reducing network bandwidth and energy power consumption requirements.

The general challenge of a routing strategy is too capable to deliver data packets all the way from the source node S to the destination node D. Although, all wireless sensor routing protocols distribute this objective, each network protocol adopts a dissimilar move toward to get it. The routing approach has an important impact on the performance of sensor networks, especially since the nodes act as source node or sink or intermediate router nodes. The major challenges that a sensor routing protocol faces are as follows: resources such as node battery power and network bandwidth constraint, high error-prone and radio shared channel. IEEE 802.15.4 WSN is organizing the collected data at a centralized server in the secured location. It will measure environmental conditions like earth climatic temperature, environmental noise and environmental pollution levels, sound, humidity, wind and enemy crossing in the country border, etc.

Motivations: For popular internet, a dedicated network router controlled by the ISPs (Internet Service Providers) exists. However, in wireless networks nodes must act both as regular sensor node such as source or sink and also as intermediate routers nodes for other sensor nodes. In the presence of centralized routers, providing network security becomes a more difficult task in the networks. Traditional legacy routing protocols for wireless networks fail to provide the required security mechanism.

Prominent existing wireless sensor routing protocols such as AODV (Ad Hoc On Demand Distance Vector) routing protocol[1], DSR (Dynamic Source Routing) protocol[2] and Low Energy Adaptive Clustering Hierarchy (LEACH) typically assume a network trusted and supportive situation. As a result, a malicious node attacker can readily become a intermediate router and interrupt network operations by deliberately disobeying the network protocol terms.

In wireless a network, data packet delivery are achieved through two closely related network layer operations includes control routing packets and data packet forwarding. As a result, the network security solution should cover the protection of both. The secure routing problem has been comprehensively researched and a number of people proposed many secured routing protocols in the literature survey discussed in the next chapter. A few of these are ARAN (Authenticated Routing for Ad Hoc Networks), SAODV (Secure Ad Hoc On-Demand Distance Vector routing) and SRP (Secured Routing Protocol). All these above protocols focus on defending the correctness of the network routing table maintained at each and every node, while leaving data packet forwarding mostly unprotected. In addition, they typically protect the routing control messages through various cryptographic attributes, resultant in a constant and nontrivial network routing overhead in terms of both network computation and network communication. On the other hand, the secure data packet forwarding problem has acknowledged relatively little interest. While Watchdog and Pathrater can diminish the harmful effects of data packet drop in the context of DSR (Dynamic Source Routing)[2], its applicability for the distance-vector routing protocols such as AODV and SAODV is not addressed yet.

Low Energy Adaptive Clustering Hierarchy (LEACH) is a TDMA based MAC (Medium Access Control) protocol which is integrated with clustering and a simple routing protocol in Wireless Sensor Networks (WSNs). The goal of LEACH[3] is to lower the energy consumption required to create and maintain clusters in order to progress the life time of a wireless sensor network. LEACH is a hierarchical protocol in which most nodes transmit to cluster heads and the cluster heads aggregate and compress the data and forward it to the base station (sink). Each node uses a stochastic algorithm at each round to determine whether it will become a cluster head in this round. LEACH assumes that each node has a radio powerful enough to directly reach the base station or the nearest cluster head but that using this radio at full power all the time would waste energy.

Nodes that have been cluster heads cannot become cluster heads again for P rounds where P is the desired percentage of cluster heads. Thereafter, each node has a 1/P probability of becoming a cluster head again. At the end of each round, each node that is not a cluster head

selects the closest cluster head and joins that cluster. The cluster head then creates a schedule for each node in its cluster to transmit its data.

All nodes that are not cluster heads only communicate with the cluster head in a TDMA fashion, according to the schedule created by the cluster head. They do so using the minimum energy needed to reach the cluster head and only need to keep their radios on during their time slot. LEACH[3] also uses CDMA, so that, each cluster uses a different set of CDMA codes, to minimize interference between clusters.

The primary difficulty is that, due to their well-built interdependency, network routing message and network data packet forwarding should be protected collectively. SCAN is more comprehensive, in the sense, that it network is monitor not only data packet dropping but also other network misbehaviors like giving wrong hop count or less hop count. ETUS[4, 5] is providing solution for network layer operation. Our motivation is to tackle the problem of securing the network layer operations from mitigating malicious nodes while minimizing, storage, computation and communication overheads.

OBJECTIVE OF THIS PAPER

It is found that the performance of a typical on demand routing protocol sharply decrease in the percentage of mitigating malicious nodes increases. The objective of the researcher's work is to provide security and obtain improved performance in the presence of malicious nodes. The researcher focuses on civilian situations and assume overheads are to be kept as minimum as possible. Thus the model does not correspond to the situation where heavily jacketed, steel helmeted and fully armed commandos are trying to protect nuclear installations but rather corresponds to a scenario where a team of local policemen, each armed with no more additional components such as a whistle and a stick control the traffic flow. Based on the above motivations security features are to be incorporated to the popular AODV protocol while limiting overheads. The following situations involving malicious nodes are to be taken care of:

- Reporting false hop count and false sequence number
- Deliberate dropping of data packets

With this perspective a enhanced triple umpiring system ETUS is proposed. ETUS not only detects malicious nodes but also salvages the network from disruptions caused by the malicious nodes. Researchers extended a solution ETUS to generic attack such as Black listing attack, Black hole attack, Byzantine attack, Changing route tables attack, Gray hole attack, Jelly fish attacks, network jamming signal, Masquerading data attack, Man in the middle attack, Replay attack, Rushing attack, Sybil attack, Selfish node attack, Sink hole attack and Worm hole attack. In second work, Intrusion Detection System for Mitigating attacks (IDSM) using Energy Monitoring (IDSEM) protocol is proposed where every node needs a token and good energy power then only nodes are allow to participate in the network and the neighboring nodes act as umpire. This proposed IDSEM is found to be very efficient with a reduced detection time and less overhead. Final work, solution for malicious node problem using the frame work approach. The conventional security frame work mechanisms like Intrusion Detection System (IDS) of network security are not enough for these networks. In this thesis, we introduce an Enhanced Intrusion Detection and Response (EIDR) system using two tire processes. The first contribution of proposed EIDR system is optimal cluster formation and performed by the Chaotic Ant Optimization (CAO) algorithm. The second contribution is to calculate the trust value of each sensor node using the Multi Objective Differential Evolution (MODE) algorithm. The computed trust value is used to design the Intrusion Response Action (IRA) system which offers additional functions and exhibit multiple characteristics of response to mitigate intrusion impacts. The simulation results display that the proposed EIDR system has a better detection rate and false positive rate without affecting network performance. Extensive simulation studies using network simulator helps to study the proposed solution soundness and prove the robustness of the system. Specific contributions are discussed in brief in the study.

Contributions: The thesis studies an important security and power issue in wireless sensor networks, i.e., the protecting the network layer operations from mitigating attacks. Malicious nodes may disturb routing algorithms by transmitting a false hop count such as lesser hop count or no route, they may drop data packets, network route the data packets through unintended routes and so on. Three studies are presented.

The first study deals with the behaviour of ETUS routing protocol in the presence of various types of generic attacks. We have conducted simulation studies to assess the improved performance of Generic ETUS over ETUS routing protocol. In this investigation, we have done these studies using AODV protocol and modified AODV protocol called as Generic ETUS. Generic attack includes Black listing attack, Black hole attack, Byzantine attack, Changing route tables attack, Gray hole attack, Jelly fish attacks, network jamming signal, Masquerading data attack, Man in the middle attack, Replay attack, Rushing attack, Sybil attack, Selfish node attack, Sink

hole attack and Worm hole attack. The results of simulation studies confirm that Generic ETUS routing protocol improves the performance of ETUS routing protocol significantly as compared with that of conventional plain AODV protocol with only nominal overheads.

The second study presents a new model to the extension of the protecting the network layer from the malicious attacks, by defining a token-based IDS technique is proposed where every node needs a token to participate in the network and the neighboring nodes act as umpire. Intrusion Detection System for Mitigating attacks (IDSM) Using Energy Monitoring (IDSEM) protocol is proposed where every node needs token and good energy powers then only nodes are allow to participate in the network and the neighboring nodes act as umpire. This proposed IDSEM is found to be very efficient with a reduced detection time and less overhead. The security analysis and experimental results have shown that IDSEM is feasible for enhancing the security and network performance of real applications. The token consists two important fields such as sensor_nodeID and sensor_status bit; sensor_nodeID is considered to be absolute. Initially the sensor_status bit of all participating nodes are "green flag" with free will to participate in all network operations includes routing and forwarding operations. When an nearby umpiring node finds its subsequent node mitigating it sends an error message to the source node S and mitigating node's status bit is changed using Flag message ("red flag"). With "red flag" on the culprit node is prohibited from participating in the any other network activities. IDSEM does not apply any cryptographic techniques on the routing and packet forwarding messages. The system concentrates only on two types of malicious attacks: giving false hop count/sequence number and dropping of the packets. We have conducted extensive simulations to evaluate the soundness of the proposed IDSEM Model.

The last study is on the extension of the IDS. Intrusion Detection System (IDS) of network security are not enough for these networks. We introduce an Enhanced Intrusion Detection and Response (EIDR) system using two tire processes. The first contribution of proposed EIDR system is optimal cluster formation and performed by the Chaotic Ant Optimization (CAO) algorithm. The second contribution is to calculate the trust value of each sensor node using the Multi Objective Differential Evolution (MODE) algorithm. The computed trust value is used to design the Intrusion Response Action (IRA) system which offers additional functions and exhibit multiple characteristics of response to mitigate intrusion impacts.

We propose a frame work Enhanced Intrusion Detection and Response (EIDR) system that provides security for routing and data forwarding operations. In our system, each node's behavior from source to destination is closely monitored by a set of three nearby nodes are called umpires. If any misbehavior is noticed, EIDR flag off the guilty node from the circuit. We have proposed three enhancements to the basic ETUS such as Link status, Token status and Battery status. Protocols have need of correct information of the link status between neighboring mobile nodes. In the token status misbehaving nodes, token status is changed. Battery life status is helpful to choose good battery strength nodes. The model with these three enhancements is called EIDR. We have implemented EIDR using LEACH protocol. Extensive investigation studies using simulator establish the soundness and robustness of the proposal. The results show that EIDR, significantly improves the performance of IDSEM and Generic ETUS in all metrics, packet delivery ratio, control overhead and end-to-end delay.

Extensive simulation studies have been performed using NS 2, a scalable simulation environment for wireless network system. The four studies on the NS 2 simulator experimental results validate the soundness of the proposal.

REVIEW OF VARIOUS ROUTING PROTOCOLS

Overview: A wireless sensor network consists of a group of wireless sensor nodes that are connected by wireless links for specified purpose. The topology in such a sensor network may rigid. Sensor routing protocols used in traditional wired networks cannot be straight applied in WSN networks due to their static topology, presence of established infrastructure for centralized administration, bandwidth constrained links and resource constrained nodes. The variety of routing protocols for wireless WSN has been proposed in the latest past. In this study, reviews the relevant literature.

Unicast routing protocols: Prominent unicast networking routing protocols for MANET can be divided into a number of routing protocol types based on dissimilar criteria. First type, routing protocols is distance vector. These protocols were originally designed for wired networks. The followings are some of DV algorithms (Distance Vector): Distributed Bellman Ford routing algorithm and Routing Internet Protocol (RIP). A pure distance vector algorithm does not perform well in wireless networks for the reason that of twin reasons of slow network convergence and count to infinity problem. The newly proposed routing protocols solve the above two problems and improve the pure DV algorithm. Enhanced routing protocols of this type comprise LRR (Least Resistance Routing), DSDV (Destination Sequence

Distance Vector) routing protocol, WRP (Wireless Routing Protocol), CGSR (Cluster-Head Gateway Switch Routing) protocol[6] and QoS Routing.

The second types of routing protocols are based on link state routing algorithms. The protocols falling in this category are GSR (Global State Routing) protocol[7], ALP (Adaptive Link State Protocol), OLSR (Optimized Link State Routing protocol), STAR (Source Tree Adaptive Routing protocol), FSR (Fisheye State Routing) protocol and LANMAR (Landmark Ad Hoc Routing) protocol.

The third type of routing protocols is reactive routing protocol (also called on demand protocol). The on-demand protocols create routes only when necessary for carrying traffic. In these routing protocols, network control overhead is very much decreased, since, periodic exchanges of route table information's are not mandatory. Several on demand routing protocols have been proposed and some of them are: LMR (Lightweight Mobile Routing protocol), DSR (Dynamic Source Routing) protocol[2], TORA (Temporarily Ordered Routing Algorithm) protocol, Associativity Based Routing protocol (ABR), (SSA) Signal Stability Based Adaptive routing protocol, Routing On demand Acyclic Multipath (ROAM) algorithm, RDMAR (Relative Distance Micro-discovery Ad Hoc Routing) protocol, AODV routing protocol[1], MDSR (Multipath Dynamic Source Routing) protocol, (FORP) Flow Oriented Routing Protocol, (RABR) Route-Lifetime Assessment Based Routing protocol, Preferred Link Based Routing Protocol (PLBR), DSR Over AODV routing (DOA) protocol[8], Neighborhood Discovery Protocol (NHDP) and (DYMO) Dynamic MANET on demand routing protocol.

Routing protocols belonging to the fourth group progress the performance of routing protocols and reduce the routing control overhead of protocol by utilizing the geographical information available as GPS[9]. The geographical information about the node position can easily be obtained without incurring large control overhead. The routing protocols falling in this category are: (LAR) Location Aided Routing protocol, (DREAM) Distance Routing Effect Algorithm for Mobility protocol, (FORP) Flow Oriented Routing Protocol, (GPSR) Greedy Perimeter Stateless Routing protocol, (ZHLS) Zone based Hierarchical Link State routing[10], (GLS) Grid Location Service routing protocol[11], MRP and Heterogeneous MANET (HMANET).

Additionally, to the above mentioned network layer routing disciplines, a few other routing protocols have been proposed[6]. Hybrid routing protocol uses table driven approach within the zone and on demand approach outside the zone. Important hybird routing protocol are: ZRP (Zone Routing Protocol) ZHLS (Zone based Hierarchical Link State) routing protocol[10] and (CEDAR) Core Extraction Distributed Ad hoc Routing protocol. The routing protocols proposed by Singh, etc., try to minimize the battery power consumption either nearby or internationally in the network in selecting routes[9]. Cluster Based Routing Protocol (CBRP) forms a set of nodes into cluster group in order to progress scalability. Some other surveys papers on routing protocols for mobile ad hoc networks[12].

Multicast routing protocols: A multicast routing protocol for wireless MANETs can be grouped into two types. First type is application type, for specific applications for which they are network designed. Protocols falling in these categories are Role Based Multicast (RBM) routing protocol[13], Content Based Multicast (CBM) routing protocol and Location Based Multicast Algorithms (LBM). The second type of application independent type/generic protocols are used for conventional network multicasting. It is further grouped into three different categories based on nature of multicast topology, Initialization and network topology maintenance approaches. The detailed classifications of multicast routing protocols can be found Siva Ram Murthy and Manoj.

The first category of protocols is based on nature of multicast topology routing algorithms. The protocols falling in these categories are Multicast Ad Hoc On-Demand Distance Vector (MAODV) Routing Protocol[14], (MCEDAR) Multicast Core Extraction Distributed Ad Hoc Routing, Bandwidth Efficient Multicast (BEMRP) Routing Protocol and (ODMRP) On-Demand Multicast Routing Protocol. An several surveys papers on multicast routing protocols for wireless mobile ad hoc networks.

The second category of multicast protocol is classified into two variants. If the group formation is initiated by the source node S, it is called a source-initiated multicast routing protocol, for example, (NSMP) Neighbor Supporting Ad Hoc Multicast Routing Protocol, Dynamic Core Based Multicast Routing (DCMP) Protocol, Content Based Multicast (CBM) protocol and Dynamic Multi-path Source Routing (DMSR) protocol. If it is initiated by the receivers group, is called a receiver-initiated multicast routing protocol, routing protocols falling in this categories are DDM (Differential Destination Multicast), Weight Based Multicast Routing Protocol (WBM), PLBM (Preferred Link Based Multicast) Routing protocol and (MMRA) Mobility-based Multicast Routing Algorithm protocol.

Final category of multicast protocols is based on the topology maintenance mechanism. Routing protocols falling in these category are Forward Group Multicasting Protocol-Receiver Advertising (FCMP-RA)[15], CAMP (Core Assisted Mesh Protocol) and Dissemination of

Multicast Aggregated State (DIMAS). There have been several surveys papers on topology maintenance multicast protocols for wireless MANETs.

Secure routing protocols: Conventional fixed wired network where dedicated centralized routers and controllers are used to monitor and control the wired network whereas in wireless mobile ad hoc networks, all nodes have two works in action. It will act as normal nodes as well as routers for other nodes[16]. In the absence of predefined infrastructure and centralized controller without dedicated routers, providing network security becomes a more challenging task in these networks. To protect the network layer in unified manner from malicious attacks several methods have been proposed in the research papers that rely on public cryptographic systems, symmetric key management or public key management and indexed hash chain mechanism.

The secure routing problem has been comprehensively researched by number of authors and a large number of secure routing protocols have been proposed in this literature survey, to name a few protocols, SAODV (Secure Ad Hoc On-Demand Distance Vector) routing protocol, (SAR) Secure aware Ad hoc Routing, (ARAN) Authenticated Routing for Ad Hoc Networks, SEAD (Secure Efficient Ad Hoc Distance) Vector Routing, Ariadne, SRP (Secured Routing Protocol) and SAODV. All these secure protocols center of attention on secure protecting the accuracy of the proactive routing table information maintained at each node while leaving the data packet forwarding typically unprotected[9].

Different types of attacks on MANET were discussed by Suresh, etc., they have designed a security mechanism by which they can minimize or completely remove many of those attacks. Sudha Rani, etc., proposed a detection and prevention of wormhole attack in stateless multicasting. Their scheme has no central administrator. They have shown that their schemes can handle wormhole attacks.

Leonidas Georgiadia, etc., made a survey of threats and possible solutions for resource allocation and cross-layer control in wireless networks. Raj, etc., proposed a solution for black hole attacks. It was implemented in prominent AODV protocol-based MANET. Tsou developed a novel scheme BDSR to avoid black hole attack based on proactive and reactive architecture. Yu, etc., proposed a solution of a distributed and cooperative black hole node detection and elimination mechanism. Solda, etc., gave a solution for blacklisting attacks; in these papers, they studied the problem of forecasting attack sources based on past attack logs from several contributors. They formulated this problem as an implicit recommendation system by Ayyaswamy, etc.

Hernandez, etc., introduced a fast model to evaluate the selfish node detection in MANET using a watchdog approach. They estimated the time of detection and the overhead of collaborative watchdog approach for detecting one selfish node. Singh, etc., implemented a security-based algorithmic approach in MANETs. In this analysis, an empirical and effective approach was pro-posed to optimize the packet loss frequency. Jyoshna, etc., proposed a solution for byzantine attacks in ad hoc networks using SMT protocol that provides a way to secure message transmission by dispersing the message among several paths with minimal redundancy. Megha and Jain[17] gave a solution for gray hole attack[16]. They use an Intrusion Detection System (IDS) to monitor the network or system[18], for selfish activities or policy violation and produce reports to a management station[9]. It takes over the sending of packets. Afterwards, the node just drops the packets to launch a (DoS) denial of service attack. If neighbor nodes that try to send packets over attacking nodes lose the connection to destination, then they may want to discover a route again by broadcasting RREQ messages by Kathirvel and Srinivasan[4, 5, 19] and Kathirvel[20].

Jayasingh and Swathi proposed a mechanism that detects the jellyfish attacks at a single node and that can be effectively deployed at all other nodes in the ad hoc network. They gave a solution that detects the jellyfish reorder attack based on the reorder density which is a basis for developing a metric.

Timothy, etc., paper focuses on jamming at the transport/network layer. Jamming at this layer exploits AODV and TCP protocols and is shown to be very effective in simulated and real networks when it can sense victim packet types but the encryption is assumed to mask the entire header and contents of the packet, so that, only packet size, timing and sequence is available to the attacker for sensing.

Kurkure and Chaudhari illustrated a comparative analysis of the selfish node detection methods based on detection time and message overhead. In this paper, a collaborative watchdog method was used to identify the selfish nodes and diminish the detection time and message overhead. Sahu and Sinha suggested a cooperative approach for understanding the behavior of IDS in MANETs. In this study, they described about various attacks and techniques used for intrusion detection which were proposed to provide high performance. Patel, etc., used an AODV protocol for trust-based routing in ad hoc networks. Ad hoc networks have limited physical security, less infrastructure, restricted power supply, mobility network and changing network topology. Jawhar, etc., suggested a reliable routing protocol for enhanced reliability and security of communication in the MANET and sensor networks.

Various P2P media streaming systems have been deployed successfully and corresponding theoretical investigations have been performed on such systems. In this study, Wang, etc., thoroughly investigates the[21] evolutionary dynamics of soft security mechanism, namely reciprocity-based incentive mechanism, in P2P systems based on Evolutionary Game Theory (EGT). By soft security mechanism, it means social control mechanisms to overcome peer's selfish (rational) behaviors and encourage cooperation in P2P systems.

Trust based routing protocols: Trust management plays an important role in IoT for reliable data fusion and mining, qualified services with context awareness and enhanced user privacy and information security. It helps people overcome perceptions of uncertainty and risk and engages in user acceptance and consumption on IoT services and applications[22]. However, current literature still lacks a comprehensive study on trust management in IoT. Authenticated key agreement protocol is a useful cryptographic primitive[18] which can be used to protect the confidentiality, integrity and authenticity for transmitted data over insecure networks.

Built upon opportunistic routing and random linear network coding, Code Pipe not only simplifies transmission coordination between nodes but also improves the multicast throughput significantly by exploiting both intra-batch and inter batch coding opportunities[23]. In particular, four key techniques, namely LP-based opportunistic routing structure[24], opportunistic feeding, fast batch moving and inter batch coding, are proposed to offer substantial improvement in throughput, energy efficiency and fairness[23].

In the study, Yen, etc., proposes a multi-constrained QoS multicast routing method using the genetic algorithm. The proposal will be flooding limited using the available resources and minimum computation time in a dynamic environment. By selecting the appropriate values for parameters such as crossover, mutation and population size, the genetic algorithm improves and tries to optimize the routes.

For the author of this study, Cheng *et al*.[22], they consider the assignment strategy with topology preservation by organizing the mesh nodes with available channels and aim at minimizing the co-channel interference in the network. The channel assignment with the topology preservation is proved to be NP-hard and to find the optimized solution in polynomial time is impossible. They have formulated a channel assignment algorithm named as DPSO-CA which is based on the discrete particle swarm optimization[24] and can be used to find the approximate optimized solution[22].

All the above schemes only try to protect the system from the attacker but not bother about quarantining attackers[25]. The TBUT systems not only detect the mischievous nodes but also prevent their further participation in the network. The twin mechanisms of watchdog and pathrater not only detect the mischievous nodes but also prevent their further participation in the network. SCAN also has similar action[24] but is more comprehensive, in the sense that not only packet dropping but also other misbehaviors like giving wrong hop count are covered[26]. Several other surveys papers on secure protocols for networks.

Intrusion detection system: Many researchers have been give variety of solution for IDS solutions in the papers[27-34]. Han *et al*.[35] have proposed Algorithm Based on Neighborhood information against sinkhole attack. The proposed algorithm includes the following three steps: Identifying suspected nodes, recognizing sinkhole nodes and eliminating sinkhole nodes. In the first stage, Identifying suspected nodes; two types of routing paths are defined to identify suspicious nodes according to the number of sensor nodes on a routing path. In the second stage, recognizing sinkhole nodes The sinkhole nodes between two communication sensor nodes are detected from the suspicious nodes based on the number of interaction times and Acknowledgments (ACKs) between the nodes. The last stage is to remove sinkhole nodes.

Lin *et al*.[36] have developed a completely unique globoid model to confirm the all-directional detection quality whereas saving the network energy effectively, that divides the sensing space into outer shell and interior region. An outer shell coverage algorithm used to assurance the recognition quality of interrupting events. Then a Markov prediction model is planned to predict the probability of motion in the adjacent area based on the intruder's historic trajectory. Based on the predicted results and using SDR technology, covered nodes will be allocated different working frequencies. The different working frequencies will be allocated to the covered nodes by a trajectory correction strategy to relocate the missing intruders during the operation.

Pintea *et al*.[37] have proposed a new generalization of agents-based systems to resolve a complex problem in wireless sensor networks, i.e., Denial Jamming Attacks. The algorithm is motivated by organic pests, ants and their behavior which uses stigmergic indirect communication. There are other mechanisms such as the sensitivity of artificial agents, the parameter used to apply direct and indirect communication also used. Agents are grouped on the basis of their sensitivity level. Agent's groups work together to solve agent's communications and problems. The presented algorithm increases the responses of agents in the network, forwarding the information when a jamming attack is exist in the wireless sensor network.

Huang *et al*.[38] have suggested an intrusion detection approach using a Hierarchical Self-Organizing Map (HSOM) neural network. It is used to study traffic patterns and detect intrusions and dynamic learning method to deal with the problem of huge and unnecessary training data. A traffic model is established to describe the dynamic features of the network traffic. By means of this traffic model, the size of training set worn for traffic pattern learning can be knowingly decreased.

Zhang *et al*.[25] have proposed intrusion detection using Dynamic State context and Hierarchical Trust (IDSHT) which is adaptable and appropriate for continually changing WSNs categorized by deviations in the perceptual environment, transitions of states of nodes and differences in trust value. They developed a multidimensional two-level hierarchical trust mechanism in the level of sensor nodes and cluster heads. They considered interactive trust, honesty trust and content trust which combines direct evaluation and feedback-based evaluation in the fixed hop range[35-44]. This means that the trust is evaluated by neighbor and base station, the complexity of evaluation is reduced. A self-adaptive dynamic trust based intrusion detection mechanism is described to improve the flexibility and applicability and is right for cluster-based WSNs.

Mrugala *et al*.[39] have proposed the automated attack generation system using genetic programming (GP) and the accreditations can be attempted sensibly. The GP passed on aggressors concentrated on publish-purchase in trades inside a WSNs that was guaranteed by a faker safe IDS. The GP aggressors alluringly secured more clear messages than the hand-coded get used at first to test the IDS while diminishing the likelihood of area. It was possible to reconfigure the IDS to animate its execution. A proof-of-control as opposed to a turnkey hypothesis, they show that GP-influenced aggressors to can connect with the endorsement of structures with clearing strike surfaces.

Sedjelmaci *et al*.[40] have proposed an ids and ejection framework against lethal attacks which sees savage ambushes with a high accuracy before they hurt the structure while thinking about the shocking position preventions of different obsession centers. The security redirection issue is controlled by a Bayesian beguilement plot. It other than made by the IDS and attackers with the outline of Impedance Release Structure (IES) and suspicious obsessions where each and every one of them finishes particular approaches to help their own particular settlements.

Guo *et al*.[41] have proposed multi-protocol oriented middleware-level intrusion detection (MP-MID) which passes on all known catch makes for any controlling custom. The managing custom with the framework Algebra for remote work structures (AWN) tongue and used the beginning of catch centers to find all catch shapes. Working up hit centers with formalized tradition in AWN to complete the co-sentences which address the catch joins into the custom. With program cutting change, all known trap makes can be found in light of co-sentences.

Santoro *et al*.[42] have proposed hybrid Network Intrusion Detection Systems (NIDS) using DEMPSTER-SHAFER (DS) theory to sympathetically watch mastermind allocator vector (NAV) ambushes. The high certification rate execution have made by signature-based NIDSs close to the noticeable strikes gave by the assortment from the standard based NIDSs. The zone justification ties the mix of evaluations from different estimations over various layers of learning with a particular monster focus to settle on a total decision on whether a NAV get happens or not[45].

Alsaedia *et al*.[43] have proposed an Energy Trust System (ETS) to effectively detect sybil attacks which uses multi-level clear insistence in setting of character and position bolster. A trust figuring is connected in setting of the centrality of each sensor center point. Data indicate is utilized to diminish correspondence overhead and extra centrality. The execution of this structure is poor down the degree that security and resource use using theoretical and redirection based procedures.

Jokhio *et al*.[16] have proposed the novel Sensor node Capture Attack Detection and Defence (SCADD) protocol. SCADD provides a cost-effective solution against the node compromise and capture attacks in WSNs, enhancing the overall WSN security for security-sensitive applications. This protocol consists of two building blocks: node attack detection block and defence advocating measure block. The former provides strategic-based attack detection to eliminate the possibility of misjudgment and the latter uses a self-destruction defence measure against node capture attack without actually destroying the node's radio service, to avoid a major security breach.

Riecker *et al*.[46] have developed three decentralized, lightweight data anomaly detection mechanisms that can be run directly on sensor nodes. These algorithms are evaluated with a real dataset to which we added plausible attacks.

Xie *et al*.[26] have proposed a new technique for handling data in a segment-based manner. Considering a collection of neighboring data segments as random variables, they determined those behaving abnormally by exploiting their spatial predict abilities and motivated by spatial analysis, specifically investigate how to implement a prediction variance detector in a WSN. As the communication cost incurred in aggregating a covariance matrix is finally optimized using the Spearman's rank correlation coefficient and differential compression, the proposed scheme is able to efficiently detect a wide range of long-term anomalies.

Zhou *et al*.[47] have proposed a suite of optimization methods to minimize the energy cost of watchdog usage while keeping the system's security in a sufficient level. Their contributions consist of theoretical analyses and practical algorithms which can efficiently and effectively schedule the watchdog tasks depending on the sensor node's locations and the target node's trustworthiness.

Han *et al*.[34] have proposed a novel IDS based on energy prediction (IDSEP) in cluster-based WSNs. The main idea of IDSEP is to detect malicious nodes based on energy consumption of sensor nodes. Sensor nodes with abnormal energy consumption are identified as malicious ones. Furthermore, IDSEP is designed to differentiate categories of ongoing DoS attacks based on energy consumption thresholds.

Shafiei *et al*.[48] have proposed two approaches to detect and mitigate such attack in WSNs. That provides a centralized approach to detect suspicious regions in the network using geostatistical hazard model. Furthermore, a distributed monitoring approach has been proposed to explore every neighborhood in the network to detect malicious behaviors.

The network layer routing protocols: The network layer unicast protocols for mobile wireless ad hoc networks can be grouped into several types based on different criteria as discussed in the study. In this study, some of prominent unicast routing protocols for network layer are detailed[49]. The routing protocols are, WRP (Wireless Routing Protocol), FSR (Fisheye State Routing) protocol, DSR protocol[2], AODV routing protocol and ZRP (Zone Routing Protocol)[14].

WRP: WRP (Wireless Routing Protocol) is a DV routing protocol for data packet radio networks. It has an objective of maintaining periodic table routing information among all nodes in the wired or wireless network. Network topology changes[43], it relies on communicating the changes to its nearby neighboring nodes which propagate all the way through the complete network[49]. Wireless Routing Protocol belongs to the category of network path finding algorithms to detect and avoidance of the 'count-to-infinity' problem which eliminate network looping situations and provide quicker path convergence when a network link failure result occurs.

AODV: AODV (Ad hoc on-Demand distance Vector) is a reactive routing protocol uses an on-demand approach for finding new routes in the, that is, a route is established only when it is required by a source node S for transmitting packets. AODV routing protocol, the source node S floods the Route Request (RREQ) packets in the entire network when a no route is between source node S and destination node D. During RREQ, it may obtain multiple routes from Source node S and Destination node D in a single route request. It will use destination sequence number (DestSeqNum) as route freshness to determine an up-to date path to the destination node D. Node updates its routing path information if the DestSeqNum received is greater that the last DestSeqNum stored in the node routing table. If any node have possess a route towards the destination node D with a greater sequence number than the RREQ packet, it unicasts a Route Reply (RREP) back to source node S. All intermediate nodes N having valid route to the destination node D, or the destination itself are allowed to send Route Reply (RREP) to the source node S[4, 5, 19, 20].

When a node in the network receives RREP control packet information about previous node from which control packets were received. It will store in the next hop towards the destination node D[50, 51]. When a link breaks it will send route error packet RERR to source node S, it will freeze the operations until identify the new path.

ZigBee is a very important technology for Wireless Sensor Networks[52-54] which is targeted at Radio-Frequency (RF) applications that require a low data rate, long battery life and secure networking. The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for ad hoc mobile networks[18]. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources. In this study, discuss about the performance of enhanced AODV in wireless sensor networks based on ZigBee[52-54].

WSN to be lower power consumption[4, 5, 19, 20], rapid topology, good real-time and so on. Above all, low power consumption bears the brunt. In order to improve the performance of the network and increase the lifetime of the network, we need to lower the power consumption of sensor node in the wireless sensor network[18]. In this study, an improved AODV routing protocol based on minimal route cost[4, 5, 19, 20, 54] is presented and OPNET is used to simulate the throughput, end-to-end delay and other parameters for evaluating the performance of the wireless sensor network with the improved protocol, the simulated results show the validation of the presented improved AODV[53].

Leach protocols: Low Energy Adaptive Clustering Hierarchy (LEACH) protocol was proposed by Heinemann, etc., is the first and prominent energy efficiency protocol for WSN. LEACH consists of two levels: cluster heads and member nodes. LEACH works on two phases: construction and communication. During construction phase cluster heads form a group. Cluster head is choose based on threshold T (n) value. Other than

cluster head node is join based on the received signal strength. The cluster head allocates the packet communication time slot for each node members based on TDMA mechanism. In the communication phase sensor nodes can send their data via. cluster head. Reserved slots are used to save energy.

Performance comparison of aodv and leach: Several comparative studies have been made between LEACH and AODV[55-60]. Though they share the on-demand behavior in that they initiate routing activities only in the presence of data packets in need of a route, several of their routing mechanics are very different. In particular, LEACH uses hierarchy based source routing where as AODV uses a table-driven routing framework and destination sequence numbers. LEACH has any TDMA based activities while AODV has the same to a certain extent. In LEACH, several additional optimizations, such as clustering mechanism, communication mechanism and less energy is used have been proposed and have been found to be very effective. The advantage of the on-demand schemes is that they do not consume large amount of network bandwidth[51]. We have chosen AODV because:

- AODV consumes less memory, compared to LEACH which consumes more memory for a route cache in cluster head
- AODV is efficient in high mobility networks but LEACH protocol is efficient only in networks with less mobility
- Source packet size in LEACH is normal, compared to AODV
- In LEACH, there is no provision for preventing routing loops
- LEACH does not have any explicit mechanism to handle stale routes in the cache or prefer fresher routes
- Power energy consumed LEACH is less as compared to AODV protocol
- LEACH throughput is slightly better than AODV. LEACH maintains a high packet delivery ratio than AODV
- In general the energy power consumption is increasing in both protocols when the simulation time increases

CONCLUSION

This study has reviewed the research works done both in unicast and multicast routing protocols. Attention has also been focused on secure network routing protocols that have been proposed. Special mention has been made about IDS which have attempted to protect the third layer from attacker's, i.e., network layer. The next chapter describes implementation of Generic ETUS protocol. This IDSEM and EIDR module is very important and is used as an add on component for the modules described in the study.

REFERENCES

01. Perkins, C.E. and E.M. Royer, 1999. Ad-hoc on-demand distance vector routing. Proceedings 2nd IEEE Workshop on Mobile Computing Systems and Applications WMCSA'99, February 25-26, 1999, IEEE, New Orleans, Louisiana, pp: 90-100.
02. Johnson, D.B. and D.A. Maltz, 1996. Dynamic source routing in Ad hoc wireless networks. Mobile Comput., 353: 153-181.
03. Varshney, S. and R. Kuma, 2018. Variants of LEACH routing protocol in WSN: A comparative analysis. Proceedings of the 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence), January 11-12, 2018, IEEE, Noida, India, pp: 199-204.
04. Kathirvel, A. and R. Srinivasan, 2011a. Double umpiring system for security of mobile Ad Hoc network. Int. J. Wireless Network Applic., 1: 151-162.
05. Kathirvel, A. and R. Srinivasan, 2011b. ETUS: Enhanced triple umpiring system for security and robustness of wireless mobile Ad hoc networks. Int. J. Commun. Networks Distrib. Syst., 7: 153-187.
06. Liu, W., C.C. Chiang, H. Wu and C. Gerla, 1997. Routing in clustered multihop, mobile wireless networks with fading channel. Proc. IEEE Sicon., 97: 197-212.
07. Chen, T.W. and M. Gerla, 1998. Global state routing: A new routing scheme for ad-hoc wireless networks. Proceedings of the International Conference on Communications, Volume 1, Jun 7-11, 1998, Atlanta, GA., pp: 171-175.
08. Bai, R. and M. Sighal, 2006. DOA: DSR over AODV routing for mobile ad hoc networks. IEEE Trans. Mobile Comput., 5: 1403-1416.
09. Rassam, M.A., A. Zainal and M.A. Maarof, 2013. Advancements of data anomaly detection research in wireless sensor networks: A survey and open issues. Sens., 13: 10087-10122.
10. Joa-Ng, M. and I.T. Lu, 1999. A peer-to-peer zone-based two-level link state routing for mobile ad hoc networks. IEEE J. Selected Areas Commun., 17: 1415-1425.
11. Li, J., J. Jannotti, J.D. Couto, D.R. Karger and R. Morris, 2000. A scalable location service for geographic Ad hoc routing. Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, August 6-11, 2000, Boston, Massachusetts, United States, pp: 120-130.

12. Broch, J., D.A. Maltz, D.B. Johnson, Y.C. Hu and J. Jetcheva, 1998. A performance comparison of multi-hop wireless ad hoc network routing protocols. Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking, October 1998, ACM, Dallas, Texas, USA., pp: 85-97.
13. Briesemeister, L. and G. Hommel, 2000. Role-based multicast in highly mobile but sparsely connected ad hoc networks. Proceedings of the 2000 1st Annual Workshop on Mobile and Ad Hoc Networking and Computing MobiHOC (Cat. No. 00EX444), August 11, 2000, IEEE, Boston, Massachusetts, pp: 45-50.
14. Royer, E.M. and C.E. Perkins, 1999. Multicast operation of the ad-hoc on-demand distance vector routing protocol. Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking, August 15-20, 1999, ACM, Seattle, Washington, pp: 207-218.
15. Chiang, C.C., M. Gerla and L. Zhang, 1998. Forwarding Group Multicast Protocol (FGMP) for multihop, mobile wireless networks. Cluster Comput., 1: 187-196.
16. Jokhio, S.H., I.A. Jokhio and A.H. Kemp, 2012. Node capture attack detection and defence in wireless sensor networks. IET. Wirel. Sensor Syst., 2: 161-169.
17. Megha, A. and Y.K. Jain, 2011. Grayhole attack and prevention in mobile Ad hoc network. Int. J. Comput. Appl., 27: 21-26.
18. Raza, F., S. Bashir, K. Tauseef and S.I. Shah, 2015. Optimizing nodes proportion for intrusion detection in uniform and Gaussian distributed heterogeneous WSN. Proceedings of the 2015 12th International Bhurban Conference on Applied Sciences and Technology (IBCAST), January 13-17, 2015, IEEE, Islamabad, Pakistan, ISBN:978-1-4799-6369-0, pp: 623-628.
19. Kathirvel, A. and R. Srinivasan, 2011c. ETUS: An enhanced triple umpiring system for security and performance improvement of mobile Ad hoc networks. Int. J. Network Manage., 21: 341-359.
20. Kathirvel, A., 2011. Single umpiring system for security and performance improvement in mobile Ad Hoc networks. IASMS J. Bus. Spectrum, 4: 30-41.
21. Jokhio, S.H., I.A. Jokhio and A.H. Kemp, 2013. Light-weight framework for security-sensitive wireless sensor networks applications. IET Wirel. Sens. Syst., 3: 298-306.
22. Chen, J., J. Li and T.H. Lai, 2013. Energy-efficient intrusion detection with a barrier of probabilistic sensors: Global and local. IEEE. Trans. Wirel. Commun., 12: 4742-4755.
23. Peng, J., T. Liu, H. Li and B. Guo, 2013. Energy-efficient prediction clustering algorithm for multilevel heterogeneous wireless sensor networks. Intl. J. Distrib. Sens. Netw., Vol. 2013.
24. Feng-Yu, L., C. Guo-Hua and L. Xiao-Ding, 2007. Ad hoc networks security mechanism based on CPK. Proceedings of the 2007 International Conference on Computational Intelligence and Security Workshops (CISW 2007), December 15-19, 2007, IEEE, Heilongjiang, China, pp: 522-525.
25. Zhang, Z., H. Zhu, S. Luo, Y. Xin and X. Liu, 2017. Intrusion detection based on state context and hierarchical trust in wireless sensor networks. IEEE. Access, 5: 12088-12102.
26. Xie, M., J. Hu and S. Guo, 2014. Segment-based anomaly detection with approximated sample covariance matrix in wireless sensor networks. IEEE. Trans. Parallel Distrib. Syst., 26: 574-583.
27. Bleda, A.L., F.J. Fernandez-Luque, A. Rosa, J. Zapata and R. Maestre, 2017. Smart sensory furniture based on WSN for ambient assisted living. IEEE. Sens. J., 17: 5626-5636.
28. Wu, J., K. Ota, M. Dong and C. Li, 2016. A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities. IEEE. Access, 4: 416-424.
29. Hoyle, B., M.M. Rau, K. Paech, C. Bonnett, S. Seitz and J. Weller, 2015. Anomaly detection for machine learning redshifts applied to SDSS galaxies. Monthly Notices Royal Astron. Soc., 452: 4183-4194.
30. Bu, S., F.R. Yu, X.P. Liu and H. Tang, 2011. Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks. IEEE. Trans. Wirel. Commun., 10: 3064-3073.
31. Bo, S., X. Shan, K. Wu and Y. Xiao, 2013. Anomaly detection based secure in-network aggregation for wireless sensor networks. IEEE Syst. J., 7: 13-25.
32. Abduvaliyev, A., A.S.K. Pathan, J. Zhou, R. Roman and W.C. Wong, 2013. On the vital areas of intrusion detection systems in wireless sensor networks. Commun. Surv. Tutorials IEEE., 15: 1223-1237.
33. Matyas, V. and J. Kur, 2013. Conflicts between intrusion detection and privacy mechanisms for wireless sensor networks. IEEE. Secur. Privacy, 11: 73-76.
34. Han, G., J. Jiang, W. Shen, L. Shu and J. Rodrigues, 2013. IDSEP: A novel intrusion detection scheme based on energy prediction in cluster-based wireless sensor networks. Inf. Secur. IET., 7: 97-105.
35. Han, G., X. Li, J. Jiang, L. Shu and J. Lloret, 2015. Intrusion detection algorithm based on neighbor information against sinkhole attack in wireless sensor networks. Comput. J., 58: 1280-1292.

36. Lin, K., T. Xu, J. Song, Y. Qian and Y. Sun, 2016. Node scheduling for all-directional intrusion detection in SDR-based 3D WSNs. IEEE. Sens. J., 16: 7332-7341.
37. Pintea, C.M., P.C. Pop and I. Zelina, 2016. Denial jamming attacks on wireless sensor network using sensitive agents. Logic J. IGPL., 24: 92-103.
38. Huang, K., Q. Zhang, C. Zhou, N. Xiong and Y. Qin, 2017. An efficient intrusion detection approach for visual sensor networks based on traffic pattern learning. IEEE. Trans. Syst. Man Cybern. Syst., 47: 2704-2713.
39. Mrugala, K., N. Tuptuk and S. Hailes, 2017. Evolving attackers against wireless sensor networks using genetic programming. IET Wirel. Sens. Syst., 7: 113-122.
40. Sedjelmaci, H., S.M. Senouci and N. Ansari, 2016. Intrusion detection and ejection framework against lethal attacks in UAV-aided networks: A bayesian game-theoretic methodology. IEEE. Trans. Intell. Transp. Syst., 18: 1143-1153.
41. Guo, Q., X. Li, G. Xu and Z. Feng, 2017. MP-MID: Multi-protocol oriented middleware-level intrusion detection method for wireless sensor networks. Future Gener. Comput. Syst., 70: 42-47.
42. Santoro, D., G. Escudero-Andreu, K.G. Kyriakopoulos, F.J. Aparicio-Navarro, D.J. Parish and M. Vadursi, 2017. A hybrid intrusion detection system for virtual jamming attacks on wireless networks. Measurement, 109: 79-87.
43. Alsaedi, N., F. Hashim, A. Sali and F.Z. Rokhani, 2017. Detecting sybil attacks in clustered wireless sensor networks based on Energy Trust System (ETS). Comput. Commun., 110: 75-82.
44. Jin, X., J. Liang, W. Tong, L. Lu and Z. Li, 2017. Multi-agent trust-based intrusion detection scheme for wireless sensor networks. Comput. Electr. Eng., 59: 262-273.
45. Harno, H.G. and I.R. Petersen, 2014. Synthesis of linear coherent quantum control systems using a differential evolution algorithm. IEEE. Trans. Automatic Control, 60: 799-805.
46. Riecker, M., A. Barroso, M. Hollick and S. Biedermann, 2012. On data-centric intrusion detection in wireless sensor networks. Proceedings of the 2012 IEEE International Conference on Green Computing and Communications, November 20-23, 2012, IEEE, Besancon, France, pp: 325-334.
47. Zhou, P., S. Jiang, A. Irissappane, J. Zhang, J. Zhou and J.C.M. Teo, 2015. Toward energy-efficient trust system through watchdog optimization for WSNs. IEEE Trans. Inform. Forensics Security, 10: 613-625.
48. Shafiei, H., A. Khonsari, H. Derakhshi and P. Mousavi, 2014. Detection and mitigation of sinkhole attacks in wireless sensor networks. J. Comput. Syst. Sci., 80: 644-653.
49. Arockiasamy, J.P., L.E. Benjamin and R.U. Vaidyanathan, 2012. Performance evaluation of multicrypt encryption mechanism. Am. J. Applied Sci., 9: 1849-1861.
50. Sundar, R. and A. Kathirvel, 2015a. Enhanced trust based delegation for load balancing in manets. Int. J. Applied Eng. Res., 10: 104-109.
51. Sundar, R. and A. Kathirvel, 2015b. Enhanced routing algorithm to reduce number of transmission in manet. Aust. J. Basic Applied Sci., 9: 142-146.
52. Kumar, A.V., S.K. Mohideen and A. Kathirvel, 2015. Performance enhanced reverse AODV routing protocol for MANETs. Middle-East J. Scient. Res., 23: 1720-1726.
53. Kumar, J.M.S.P.J., A. Kathirvel, N. Kirubakaran, P. Sivaraman and M. Subramaniam, 2015. A unified approach for detecting and eliminating selfish nodes in MANETs using TBUT. EURASIP J. Wireless Commun. Networking, Vol. 2015. 10.1186/s13638-015-0370-x
54. Kumar, J.J. and A. Kathirvel, 2018. Optimum power management in mobile ad-hoc networks. J. Eng. Sci. Technol., 13: 1805-1815.
55. Kalkha, H., H. Satori and K. Satori, 2016. Performance evaluation of AODV and LEACH routing protocol. Adv. Inf. Technol. Theory Appl., 1: 112-118.
56. Hamela, K. and A. Kathirvel, 2018. EIMO-ESOLSR: Energy efficient and security based model for OLSR routing protocol in mobile Ad Hoc network. IET Commun., 5: 1-9.
57. Bai, R. and M. Singhal, 2005. Salvaging route reply for on-demand routing protocols in mobile ad-hoc networks. Proceedings of the 8th ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems, October 2005, ACM, New York, USA., pp: 53-62.
58. Amicarelli, A., G. Leuzzi and P. Monti, 2012. Lagrangian micromixing models for concentration fluctuations: An overview. Am. J. Environ. Sci., 8: 577-590.
59. Deif, D.S. and Y. Gadallah, 20117. An ant colony optimization approach for the deployment of reliable wireless sensor networks. IEEE. Access, 5: 10744-10756.
60. Wei, M. and K. Kim, 2012. Intrusion detection scheme using traffic prediction for wireless industrial networks. J. Commun. Networks, 14: 310-318.