A Novel Study on Privacy Scheduling Data Attacks in Hierarchical WSN

S. Saranya
Research Scholar
Department of Computer Science
Muthayammal College of Arts & Science, Namakkal, Tamilnadu.

A. Anusha Priya
Associate Professor
Department of Computer Science
Muthayammal College of Arts & Science, Namakkal, Tamilnadu.

Abstract

A wireless sensor network is a collection of numerous sensors distributed on an area of interest to collect and process data from the environment. One particular threat in wireless sensor networks is node compromise attacks, that is, attacks where the adversary gets physical access to a node and to the programs and keying material stored on it. In this Paper Privacy and energy efficiency are critical concerns in wireless sensor network (WSN) design. This paper aims to develop an energy-efficient secure scheme against power exhausting attacks, especially the denial-of-sleep attacks, which can shorten the lifetime of WSNs rapidly. Although various Medium access control (MAC) protocols have been proposed to save the power and extend the lifetime of WSNs, the existing designs of MAC protocol are insufficient to protect the WSNs from denial-of-sleep attacks in MAC layer. This is attributed to the fact that the well-known privacy mechanisms usually awake the sensor nodes before these nodes are allowed to execute the privacy processes. Therefore, the practical design is to simplify the authenticating process in order to reduce the energy consumption of sensor nodes and enhance the performance of the MAC protocol in countering the power exhausting attacks. This paper proposes a cross-layer design of secure scheme integrating the MAC protocol. The analyses show that the proposed scheme can counter the replay attack and forge attack in an energy-efficient way. The detailed analysis of energy distribution shows a reason-able decision rule of coordination between energy conservation and privacy requirements for WSNs.

Keywords: Wireless sensor networks, energy efficiency, denial-of-sleep, TCP, MAC

I. INTRODUCTION

Simple to solve you might say, as many of these security aspects have solutions in traditional networks, solutions that are well understood and used in the Internet today. These security solutions consider that the cryptographic keys are kept secret since either access to the computers is limited or tamper-proof hardware is used. When needed, for example for authenticating messages that have many receivers, public key cryptography can be used. However, in a wireless sensor network, the sensors are usually small and resource constrained devices that are placed in unattended environments. The unattended environment makes it possible for adversaries to perform node compromise attacks, that is, the adversary gets physical access to a node and to the programs and keying material stored on it. The sensors also have severe resource and power limitations which limits the choice of cryptographic protocols that can be used. The node compromise attack and the limited choice of cryptographic protocols call for novel security solutions for sensor networks.

The usages of mobile devices introduce new challenges since the users carrying the device risk exposing their locations when their device is used in the network. For example, if a user's device is used as the sink, then nodes have to be able to send data to it, or, if the device collects data about the environment, the data is usually labeled with the location. The research topics addressed in this thesis are query authentication, confidential and integrity preserving data aggregation and privacy-preserving data collection for both mobile sinks and mobile sensors. We propose a layered key distribution scheme to be used for both query authentication and confidential data aggregation supporting both static and mobile sinks.In energy consumption and extend the lifetime of WSNs, several schemes have been proposed. Most of the researchers aim at layer-2 protocol design. The duty-cycle based protocol is one of the major schemes in energy conservation of WSNs. In the duty-cycle based WSN MAC protocols, the sensor nodes are switched between awake/active and sleep state periodically and these nodes enter sleep mode after certain idle period. In the Low Power Listening (LPL) based WSN MAC protocol, such as B-MAC, the receiver wakes up periodically to sense the preamble from the sender and then to receive and process the data. When the sender needs to send data, it sends a long preamble to cover the sleep period to ensure the receiver waking up and sensing. The LPL based MAC protocol is an asynchronous protocol, which decouples the sender and receiver with time synchronization. This long preamble design of LPL based protocol consumes the major energy of both sender and receiver. Depending on the different initiator, the duty-cycle scheme can be classified into two types: sender-initiated scheme and receiver-initiated (RI) scheme. For instance, the X-MAC protocol is one of the sender-initiated schemes to improve B-MAC protocol by replacing the long preamble with short preambles, which allows the receiver to send acknowledgment (ACK) back to the sender as soon as it senses the preamble. The RI-MAC protocol is one of the receiver-initiated schemes to minimize the channel occupancy time of a pair of a sender and receiver, which allows the sender to send data to the receiver as soon as it senses the beacon. However, current layer-2 protocol designs are insufficient to protect a WSN from Denial-of-Sleep

attack. The energy conservation is one of the major goals of WSN design, whereas the privacy scheme always consumes more energy of system. There is no well decision rule to compromise the requirements between energy conservation and privacy scheme.

The Denial-of-Sleep is one of the power exhausting attacks of WSNs. This attack is a special type of Denial-of-Service (DoS) attack, which tries to keep the sensor nodes awake to consume more energy of the constrained power supply. An anti-node can send fake data packets to sensor node of unprotected WSNs to initiate unnecessary transmissions repeatedly. Without privacy mechanism, an anti-node can broadcast a fake preamble frequently in the sender-initiated schemes. If the receiver cannot tell the real preamble and the fake one, the receiver will receive and process the data from the anti-node. Such attack will keep the receiver awake as long as the data transmission sustains, which exhausts the battery of nodes rapidly. Moreover, an anti-node can replay a fake preamble ACK to the sender. Thus, the sender will start to send the data to the anti-node but it will never receive the right data ACK. Similarly, the sender may send data repeatedly and exhausts the battery of node rapidly. In receiver-initiated schemes, an anti-node can broadcast a "fake beacon" to cheat sender to process and send the data to the anti-node but it will never receive the right data ACK. An anti-node can replay a "fake beacon ACK" to the receiver. Thus, the receiver will start to receive and process the data from the anti-node. If the interval of attack packets is shorter than the sleep period of a WSN, then the communication between neighboring nodes in a WSN could be interfered by attack packets. Consequently, no packets from the attacked nodes can be delivered, which causes a jamming-like scenario. However, unlike the physical jamming attack, no consecutive signals or packets are needed for the packet attack. A well-designed periodical attack packet can be applied to perform such jamming-like attack, which may degrade the performance of a duty-cycle scheme for WSN operating and achieve energy conservation of an anti-node during the attack. As a result, the sender and receiver need mutual authentication schemes to counter such an attack.

In conventional wireless privacy mechanisms, the transmit-ted data is encrypted with keyed symmetric or asymmetric encryption algorithm. The wireless sensor networks prefer the symmetric algorithm to avoid the complicated computing and heavy energy consumption. But the encrypted data makes the battery exhaustion even worse under Denial-of-Sleep attack. The anti-node can send the encrypted "garbage" data to receiver. This attack forces the receiver to decrypt the data. Before the receiver identifies that the data is "garbage", the receiver consumes more power to receive and decrypt data. These processes also keep sensor nodes awake longer. Accordingly, an easy and fast mutual authentication scheme is needed to integrate with MAC protocol to counter the Denial-of-Sleep attack.In any adopted privacy mechanism of WSNs, the sensor nodes must be waked before receiving data and checking privacy properties. The practical design is to simplify the privacy process when suffering the power exhausting attacks. The design of privacy scheme in upper layers may be coupled with the fixed data link layer mechanism. In this paper, a cross-layer design of secure scheme integrating the MAC protocol, Two-Tier Energy-Efficient Secure Scheme (TE2 S), is proposed to protect the WSNs from the above attacks based on our preliminary frameworks. This cross-layer design involves coupling two layers at design time without creating new interface for information sharing at runtime. This paper proposes a two-tier secure transmission scheme. This scheme uses the hash-chain to generate the dynamic session key, which can be used for mutual authentication and the symmetric encryption key. The only computations of dynamic session key are the hash functions, such as MD5 or SHA-1, which are very simple and fast. By integrating with MAC protocol, there is no extra packet compared with the existing MAC designs. The two-tier design can check and interrupt the attacks at different check points. The combination of low complexity privacy process and multiple check points design can defense against attacks and send the sensor nodes back to sleep mode as soon as possible. The privacy analysis shows that this scheme can counter the replay attack and forge attack, and the energy analysis shows that this scheme is energy efficient as well. The detailed energy distribution of energy analysis also shows a new possible decision rule to compromise the needs between energy conservation and privacy scheme.

II. EXISTING SYSTEM

The Existing Method, current layer-2 protocol designs are insufficient to protect a WSN from Denial-of-Sleep attack. The energy conservation is one of the major goals of WSN design, whereas the privacy scheme always consumes more energy of system. There is no well decision rule to compromise the requirements between energy conservation and privacy scheme. The Denial-of-Sleep is one of the power exhausting attacks of WSNs. This attack is a special type of Denial-of-Service (DoS) attack, which tries to keep the sensor nodes awake to consume more energy of the constrained power supply. An anti-node can send fake data packets to sensor node of unprotected WSNs to initiate unnecessary transmissions repeatedly. Without privacy mechanism, an anti-node can broadcast a fake preamble frequently in the sender-initiated schemes. If the receiver cannot tell the real preamble and the fake one, the receiver will receive and process the data from the anti-node. Such attack will keep the receiver awake as long as the data transmission sustains, which exhausts the battery of nodes rapidly.

A. Drawbacks

Time taken will be high while data traveling in a long distance. Data transferring cost will be high. There is no privacy so the attacker can easily attack the data. Efficient algorithm will not be used. Replication attacks using resources.

III. PROPOSED SYSTEM

This paper aims to develop an energy-efficient secure scheme against power exhausting attacks, especially the denial-of-sleep attacks, which can shorten the lifetime of WSNs rapidly. Although various media access control (MAC) protocols have been

proposed to save the power and extend the lifetime of WSNs, the existing designs of MAC protocol are insufficient to protect the WSNs from denial-of-sleep attacks in MAC layer. This is attributed to the fact that the well-known privacy mechanisms usually awake the sensor nodes before these nodes are allowed to execute the privacy processes. In any adopted privacy mechanism of WSNs, the sensor nodes must be waked before receiving data and checking privacy properties. The practical design is to simplify the privacy process when suffering the power exhausting attacks. The design of privacy scheme in upper layers may be coupled with the fixed data link layer mechanism. In this paper, a cross- layer design of secure scheme integrating the MAC protocol, Two-Tier Energy-Efficient Secure Scheme (TE2 S), is proposed to protect the WSNs from the above attacks based on our preliminary frameworks. This cross-layer design involves coupling two layers at design time without creating new interface for information sharing at runtime.

In order to achieve integrity and at the same time aggregate data, we consider nodes verifying the aggregation result. Several protocols work in the presence of n compromised nodes, where n is a security parameter of the system. When more than n nodes are compromised, data integrity is no longer guaranteed. Chan et al. propose a protocol for provably secure hop-by-hop in network aggregation that guarantees the detection of any manipulation of aggregated data in the presence of an arbitrary number of compromised nodes. The algorithm induces low node congestion, which is the maximum communication load on any node that is further reduced by Frikken and Dougherty. Nevertheless, we have identified cases where the node congestion is higher than the one of non-aggregation protocols. The total energy consumption of the system is also in many scenarios higher than the one of non-aggregation protocols. As data aggregation is used to reduce the energy consumption in the system when collecting data, the cost of data integrity is too high in the identified cases. We work on reducing the energy consumption of the protocol proposed by Chan et al. to a level below the energy consumption of a non-aggregation scheme.

A. Algorithm-Multipath-Routing-Algorithm

Multipath routing is the routing technique of using multiple alternative paths through a network, which can yield a variety of benefits such as fault tolerance, increased bandwidth, or improved privacy. The multiple paths computed might be overlapped, edge-disjointed or node-disjointed with each other.

B. Connection Establishment between Terminals

After the server is waiting, a client instantiates a Socket object, specifying the server name and port number to connect to the constructor of the Socket class attempts to connect the client to the specified server and port number. If communication is established, the client now has a Socket object capable of communicating with the server. On the server side, the accept method returns a reference to a new socket on the server that is connected to the client's socket.

After the connections are established, communication can occur using I/O streams. Each socket has both an Output Stream and an Input Stream. The client's Output Stream is connected to the server's Input Stream, and the client's Input Stream is connected to the server's Output Stream. TCP is a two way communication protocol, so data can be sent across both streams at the same time. In this paper utilizing multipath routing to answer user queries in the presence of unreliable and malicious nodes. The key concept of our redundancy management is to exploit the tradeoff between energy consumption vs. the gain in reliability, timeliness, and privacy to maximize the system useful lifetime. We formulate the tradeoff as an optimization problem for dynamically determining the best redundancy level to apply to multipath routing for intrusion tolerance so that the query response success probability is maximized while prolonging the useful lifetime. Furthermore, we consider this optimization problem for the case in which a node distributed intrusion detection algorithm is applied to detect and evict malicious nodes. We develop a novel probability model to analyze the best redundancy level in terms of path redundancy and source redundancy, as well as the best intrusion detection settings in terms of the number of voters and the intrusion invocation interval under which the lifetime of node is minimized. We then apply the analysis results obtained to the design of a dynamic redundancy management algorithm to identify and apply the best design parameter settings at runtime in response to environment changes, to maximize the WSN lifetime.

In Sockets provide the communication mechanism between two computers using TCP. A client program creates a socket on its end of the communication and attempts to connect that socket to a server. When the connection is made, the server creates a socket object on its end of the communication. The client and server can now communicate by writing to and reading from the socket. The java.net. Socket class represents a socket, and the java.net. Server Socket class provides a mechanism for the server program to listen for clients and establish connections with them. The following steps occur when establishing a TCP connection between two computers using sockets. The server instantiates a Server Socket object, denoting which port number communication is to occur on. The server invokes the accept method of the Server Socket class. This method waits until a client connects to the server on the given port.

IV. SECURITY IN MOBILE NETWORKING

Computer security deals with prevention, detection and survivability of attacks. As sensor networks are commonly deployed in unattended environments, it is common to focus on the survivability of attacks, that is, coping with some attack and still function normally. We list common security requirements that are needed in order to achieve security:

– Confidentiality or privacy is defined as the prevention of unauthorized access to information. A violation of the confidentiality results in information disclosure.

- Integrity is defined as the prevention of unauthorized, either accidental or malicious, modification or destruction of information. Data modification or deletion would result in deceiving the authorized entity by providing him with false information.
- Authentication – Entity authentication is defined as the process of verifying an entity's claimed identity, while data origin authentication is defined as the process of verifying the originator of the data, which implies data integrity.
- Availability – Availability refers to the percentage of time a system is working and available to the user. In the context of a sensor network it refers to the ability to collect data from the sensors. It is not directly a security requirement, nevertheless as an adversary can mount different attacks to interfere with the normal functionality of the sensor network, we consider it as part of the security requirements.
- Data freshness – An adversary should not be able to reuse old authentic Messages

This section describes the wireless model that was originally ported as CMU's Monarch group's mobility extension to NS2. The first section covers the original mobility model ported from CMU/Monarch group. In this section, we cover the internals of a mobile node, routing mechanisms and network components that are used to construct the network stack for a mobile node. The components that are covered briefly are Channel, Network interface, Radio propagation model, MAC protocols, Interface Queue, Link layer and Address resolution protocol model (ARP). CMU trace support and Generation of node movement and traffic scenario files are also covered in this section. The original CMU model allows simulation of pure wireless LANs or multihop ad-hoc networks. Further extensions were made to this model to allow combined simulation of wired and wireless networks. MobileIP was also extended to the wireless model.

A. The Basic Wireless Model in NS

The wireless model essentially consists of the MobileNode at the core, with additional supporting features that allows simulations of multi-hop ad-hoc networks, wireless LANs etc. The MobileNode object is a split object. The C++ class MobileNode is derived from parent class Node. A MobileNode thus is the basic Node object with added functionalities of a wireless and mobile node like ability to move within a given topology, ability to receive and transmit signals to and from a wireless channel etc. A major difference between them, though, is that a MobileNode is not connected by means of Links to other nodes or mobilenodes. In this section we shall describe the internals of MobileNode, its routing mechanisms, the routing protocols dsdv, aodv, tora and dsr, creation of network stack allowing channel access in MobileNode, brief description of each stack component, trace support and movement/traffic scenario generation for wireless simulations.

V. WIRELESS SENSOR NETWORK

WSNs to take the intermittent connectivity and time-varying topology into Consideration. WSNs mainly focuses on routing .nodes store the packets in their buffers if there is no opportunity for message forwarding and wait for future opportunities. Then the key problem is how to select appropriate relay nodes for message forwarding during encounters. Two types of solutions are used in WSN routing: single-copy or flooding based. In single-copy WSN routing, there is only one copy of each message in the network at any time so that the resulting propagation path of a message is a single path from the source to the destination. To make the right routing decision (i.e., picking the right relay at each step), a good metric to measure the ability of nodes to deliver the message is essential.

A. Transmission Control Protocol

The Transmission Control Protocol (TCP) is a core protocol of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP. TCP provides reliable, ordered, and error-checked delivery of a stream of octets between applications running on hosts communicating over an IP network. TCP is the protocol that major Internet applications such as the World Wide Web, email, remote administration and file transfer rely on. Applications that do not require reliable data stream service may use the User Datagram Protocol (UDP), which provides a connectionless datagram service that emphasizes reduced latency over reliability. The Transmission Control Protocol provides a communication service at an intermediate level between an application program and the Internet Protocol. It provides host-to-host connectivity at the Transport Layer of the Internet model. An application does not need to know the particular mechanisms for sending data via a link to another host, such as the required packet fragmentation on the transmission medium. At the transport layer, the protocol handles all handshaking and transmission details and presents an abstraction of the network connection to the application.

B. User Devices as Sensor Nodes

Mobile devices can nowadays be used as sensor nodes, which make it easier to collect data as no sensor deployment is necessary. As the users move in their day to day life, their devices sense the environment and collect data. The data is reported in form of events to the sink, which in this case is referred to as a system server. As the users move over time, the data they report has to be tagged with location information in order to be useful for the server. An event will therefore include location information, time and service related information, i.e., sensed data. The events of a user u form the user's trace in the system. We are concerned with adversaries that want to find out where different users are or trace users during different periods of time. From the location

information, adversaries can infer personal information about a user, like which health institutions are visited and other personal visits.

While IP handles actual delivery of the data, TCP keeps track of the individual units of data transmission, called segments that a message is divided into for efficient routing through the network. For example, when an HTML file is sent from a web server, the TCP software layer of that server divides the sequence of octets of the file into segments and forwards them individually to the IP software layer (Internet Layer). The Internet Layer encapsulates each TCP segment into an IP packet by adding a header that includes (among other data) the destination IP address. When the client program on the destination computer receives them, the TCP layer (Transport Layer) reassembles the individual segments, and ensures they are correctly ordered and error free as it streams them to an application.

VI. CONCLUSION

This paper proposes a cross-layer design of energy-efficient secure scheme integrating the MAC protocol. No extra packet is involved in the original MAC protocol design. This scheme can reduce the authenticating process as short as possible to mitigate the effect of the power exhausting attacks. By combination of low complexity privacy process and multiple check points, the proposed design can defense against attacks and send the sensor nodes back to sleep mode as soon as possible. The privacy analysis shows that this scheme can counter the replay attack and forge attack. The energy analysis identifies the operating mode precisely, including the MCU and radio modules. The simulation results of normalized energy consumption for normal condition, which has no attacks, show that the proposed scheme increases less than 2.57% in energy consumption of the X-MAC protocol and less than 3.63% in energy consumption of the RI-MAC protocol with varying packet sending rates. The simulation results of normalized energy consumption for attack conditions also show that the proposed scheme can save times of energy consumptions than X-MAC or RI-MAC does, which also can extend the lifetime of WSNs under attacks. The energy analysis shows that this scheme is efficient in both sender-initiated scheme and receiver-initiated scheme. The overall results show that the proposed secure TE 2 S scheme can achieve the same throughput performance with less energy consumption. Further energy consumption of the proposed scheme under various duty cycles can be investigated to provide more extensive simulation results to support the efficiency of TE 2 S scheme in the future.

REFERENCES

[1] A.Anusha Priya, Lavanya.C, Enhanced Focus on User Revocation in Secure Dynamic Auditing For Data Storage in Cloud, 2016/8, International Journal of Emerging Technology in Computer Science & Electronics, Volume 23, Issue 4, Pages 51-55.
[2] G.Naveena, A.Anusha Priya, A Certain Investigation on Cluster Based Medium Access Control and QoS Aware Routing Protocol for Heterogeneous Networks, 2016, International Journal for Scientific Research & Development, Volume 4, Issue 7, Pages 1117-1122.
[3] S.Yasmin, A.Anusha Priya, Decentralized Entrance power with Secret Endorsement of data Stored in Clouds, 2015/8, International Journal of Innovative research in Computer and Communication Engineering, Volume 3, Issue 8, Pages 7279-7284.
[4] A.Anusha Priya G.Vijayalakshmi, Perceiving Kernel-Level Rootkits Using Data Structure Invariants, 2015/7, International Journal of Innovative Research in Computer and Communication Engineering, Volume 3, Issue 7, Pages 6719-6724.
[5] N.Thavamani, A.Anusha Priya, A QOD-Slanting Scattered Steering Procedure for Fusion Wireless Set of Connections, 2015/7, International Journal of Innovative Research in Computer and Communication Engineering, Volume 3, Issue 7, Pages 6752-6757.
[6] M.Ravi A.M.Nirmala, P.Subramaniam, A.Anusha Priya, Enriched Performance on Wireless Sensor Network using Fuzzy based Clustering Technique, 2013, International Journal of Advanced Studies in Computer Science and Engineering, Volume 2, Issue 3, Pages 11-17.
[7] A Anusha Priya, A Mohanapriya, An Effective Scrutiny of Static and Dynamic Load Balancing In Cloud, August 2016, International Journal of Emerging Technology in Computer Science & Electronics, Volume 23 Issue 4, Pages – 27 -30.
[8] P.Vijayakumar, A.Anusha Priya, Stabilize the Movement of Nodes on anycast Routing with jamming responsive in mobile ad-hoc networks, September 2015, international Journal of Engineering Sciences & Research Technology, Volume 4 Issue 9,Pages – 207 -214.
[9] M.Balaji, E.Aarthi, K.Kalpana, B.Nivetha, D.Suganya "Adaptable and Reliable Industrial Security System using PIC Controller" 2017/5, Journal International Journal for Innovative Research in Science & Technology, Volume 3, Issue 12, Page 56-60.
[10] A.S.Syed Navaz, C.Prabhadevi & V.Sangeetha"Data Grid Concepts for Data Security in Distributed Computing" January 2013, International Journal of Computer Applications, Vol 61 – No 13, pp 6-11.
[11] A.S.Syed Navaz, A.S.Syed Fiaz, C.Prabhadevi, V.Sangeetha & S.Gopalakrishnan "Human Resource Management System" Jan – Feb 2013, International Organization of Scientific Research Journal of Computer Engineering, Vol 8, Issue 4, pp. 62-71.
[12] A.S.Syed Navaz, S.Gopalakrishnan & R.Meena "Anomaly Detections in Internet Using Empirical Measures" February 2013, International Journal of Innovative Technology and Exploring Engineering, Vol 2 – Issue 3. pp. 58-61.
[13] A.S.Syed Navaz & G.M. Kadhar Nawaz, "Ultra-Wideband on High Speed Wireless Personal Area Networks" August – 2014, International Journal of Science and Research, Vol No – 3, Issue No – 8, pp.1952-1955.
[14] A.R. Beresford and F. Stajano. Mix zones: user privacy in location-aware services. In Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004, pages 127 – 131, March 2004.
[15] E.-O. Blaß, J. Wilke, and M. Zitterbart. Relaxed authenticity for data aggregation in wireless sensor networks. In Proceedings of the 4th International Conference on Security and Privacy in Communication Networks, SecureComm '08, pages 4:1–4:10, New York, NY, USA, 2008. ACM.
[16] J. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, and M. B. Srivastava. Participatory sensing. In Workshop on World-Sensor-Web (WSW '06): Mobile Device Centric Sensor Networks and Applications, pages117–134, 2006.
[17] J. Burrell, T. Brooke, and R. Beckwith. Vineyard computing: Sensor networks in agricultural production. IEEE Pervasive Computing, 3(1):38–45, January 2004.55
[18] A.S.Syed Navaz & Dr.G.M. Kadhar Nawaz & A.S.Syed Fiaz "Slot Assignment Using FSA and DSA Algorithm in Wireless Sensor Network" October – 2014, Australian Journal of Basic and Applied Sciences, Vol No –8, Issue No –16, pp.11-17.
[19] A.S.Syed Navaz, J.Antony Daniel Rex, S.Jensy Mary. "Cluster Based Secure Data Transmission in WSN" July – 2015, International Journal of Scientific & Engineering Research, Vol No - 6, Issue No - 7, pp. 1776 – 1781.

[20] A.S.Syed Navaz, J.Antony Daniel Rex, P.Anjala Mary. "An Efficient Intrusion Detection Scheme for Mitigating Nodes Using Data Aggregation in Delay Tolerant Network" September – 2015, International Journal of Scientific & Engineering Research, Vol No - 6, Issue No - 9, pp. 421 – 428.
[21] J.N. Al-Karaki and A.E. Kamal. Wireless Communications, IEEE, 11(6):6 – 28, December 2004.
[22] F. Armknecht, J. Girao, M. Stoecklin, and D. Westhoff. Re-visited: Denial of service resilient access control for wireless sensor networks. In Third European Workshop on Security and Privacy in Ad hoc and Sensor Networks, Hamburg, Germany, September 2006. ESAS2006. Held in conjunction with ESORICS 2006.
[23] A.S.Syed Navaz, P.Jayalakshmi, N.Asha. "Optimization of Real-Time Video Over 3G Wireless Networks" September – 2015, International Journal of Applied Engineering Research, Vol No - 10, Issue No - 18, pp. 39724 – 39730.
[24] Z. Benenson, L. Pimenidis, F. C. Freiling, and S. Lucks. Authenticated query flooding in sensor networks. In PERCOMW '06: Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, page 644, Washington, DC, USA, 2006. IEEE Computer Society.
[25] A. R. Beresford and F. Stajano. Mix zones: User privacy in location-aware services. In Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, PERCOMW '04, pages 127–, Washington, DC, USA, 2004. IEEE Computer Society.
[26] A.S.Syed Fiaz, N.Asha, D.Sumathi & A.S.Syed Navaz "Data Visualization: Enhancing Big Data More Adaptable and Valuable" February – 2016, International Journal of Applied Engineering Research, Vol No - 11, Issue No - 4, pp.–2801-2804.
[27] A.S.Syed Navaz & Dr.G.M. Kadhar Nawaz "Flow Based Layer Selection Algorithm for Data Collection in Tree Structure Wireless Sensor Networks" March – 2016, International Journal of Applied Engineering Research, Vol No - 11, Issue No - 5, pp.–3359-3363.
[28] A.S.Syed Navaz & Dr.G.M. Kadhar Nawaz "Layer Orient Time Domain Density Estimation Technique Based Channel Assignment in Tree Structure Wireless Sensor Networks for Fast Data Collection" June - 2016, International Journal of Engineering and Technology, Vol No - 8, Issue No - 3, pp.–1506-1512.
[29] M.Ravi & A.S.Syed Navaz "Rough Set Based Grid Computing Service in Wireless Network" November - 2016, International Research Journal of Engineering and Technology, Vol No - 3, Issue No - 11, pp.1122– 1126.
[30] A.S.Syed Navaz, N.Asha & D.Sumathi "Energy Efficient Consumption for Quality Based Sleep Scheduling in Wireless Sensor Networks" March - 2017, ARPN Journal of Engineering and Applied Sciences, Vol No - 12, Issue No - 5, pp.–1494-1498.
[31] A.S.Syed Fiaz, I.Alsheba & R.Meena "Using Neural Networks to Create an Adaptive Character Recognition System", Sep 2015, Discovery - The International Daily journal, Vol.37 (168), pp.53-58.
[32] AroundMe. www.aroundmeapp.com, June 2012. E. Becher, Z. Benenson, and M. Dornseif. Tampering with motes: Real-world physical attacks on wireless sensor networks. In Proceeding of the 3rd International Conference on Security in Pervasive Computing (SPC), pages 104–118, 2006.
[33] Z. Benenson, N. Gedicke, and O. Raivio. Realizing robust user authentication in sensor networks. In Workshop on Real-World Wireless Sensor Networks (REALWSN), Stockholm, Sweden, 2005.
[34] A.S.Syed Fiaz, M. Usha and J. Akilandeswari "A Brokerage Service Model for QoS support in Inter-Cloud Environment", March 2013, International Journal of Information and Computation Technology, Vol.3, No.3, pp 257-260.
[35] A.S.Syed Fiaz, R.Pushpapriya, S.Kirubashini & M.Sathya "Generation and allocation of subscriber numbers for telecommunication", March2013, International Journal of Computer Science Engineering and Information Technology Research, Vol No: 3; Issue No: 1, pp. 257-266.
[36] A.S.Syed Fiaz, N.Devi, S.Aarthi "Bug Tracking and Reporting System", March 2013, International Journal of Soft Computing and Engineering, Vol No: 3; Issue No: 1, pp. 257-266.
[37] M. Usha, J. Akilandeswari and A.S.Syed Fiaz "An efficient QoS framework for Cloud Brokerage Services", Dec. 2012, International Symposium on Cloud and Service Computing, pp: 76-79, 17-18, IEEE Xplore.