SURVEY PAPER

SECURITY ATTACKS IN WIRELESS SENSOR NETWORKS – A STUDY

By

K. THAMIZHMARAN

Department of Electronics and Communication Engineering, Government College of Engineering, Bodinayakkanur, Theni, Tamilnadu, India.

Date Received: 28/07/2020 *Date Revised: 04/08/2020* *Date Accepted: 10/08/2020*

ABSTRACT

A recent development in hardware platform shows the popularity of miniaturized devices, computational power and large connectivity. Generally, Wireless sensor network nodes are stricken by different attacks during the transmission of messages such as HELLO flood attack and Wormhole attack which causes unsystematic behavior of the nodes. This malicious behavior creates incorrect traffic and the network may experience redundancy and topology problems. The existing system is not much efficient due to the lacking of flow, error control and reliability. The survey paper gives a better solution to achieve flexible bandwidth, energy resource complications for recent communication protocols by finding malicious node. The node that produces any one of the following attack is called as malicious node. The analysis of nodes is done under various environments such as indoor, outdoor models in rural and urban areas with reference to the ISM Band which was allocated by FCC.

Keywords: Network security, Routing protocol, QoS, WSN, Computer security, Cryptography.

INTRODUCTION

Recent advances in wireless sensor networks and embedding microchips have empowered another age of enormous scale sensor systems appropriate for a scope of business and military applications. Not at all like current data administrations, for example, those on the web where data can without much of a get stale or be pointless in light of the fact that it is excessively conventional sensor systems guarantee, making it impossible to couple end client specifically to sensor estimations and give data that is decisively restricted in time/space, as indicated by the clients need or request (Lamport et al., 2019). A sensor network is liable to a remarkable arrangement of asset limitations, for example, limited on-board battery power and restricted system correspondence data transmission. Every node is likewise furnished with at least one detecting devices, for example, cameras, vibration, temperature and acoustic amplifier arrays. Sensor networks expand the current web profound into the physical condition as show in Figure 1. Data gathered by and transmitted on a sensor network portrays state of physical condition. A router routes client questions or instructions to fitting nodes in a sensor network (Liu& Singh, 1999, 2001; Kaur & Kumar, 2020). At least one information DB devices might be appended to IP network to file sensor information from various edge sensor networks. The main difficulties in routing protocol faces secured transmission, hidden terminal issues, activity, error state, bandwidth requirements and versatility of nodes. Error Prone shared radio channel necessitates that AODV associates with the MAC layer to discover the path of action through better quality connections. Likewise transmissions in AODV result in impacts of information and control packets. This prompts the hidden terminal issue. Plenty of sensors are used in various fields, for example, used in agriculture for monitoring the growth of crops, and remote wireless sensors are used to discover animals. Suitable path is required to transmit proper signals then the network needs to find paths with less congestion (Doherty,2001). The power consumption by the nodes is an important parameter. Efficient utilization of energy will increase the lifetime of network.

1. Network Security Attacks

Adhoc Transport Protocol (ATP) is exceptionally proposed for adhoc wireless networks and is certainly not a variation of TCP. The significant aspects by which ATP concedes

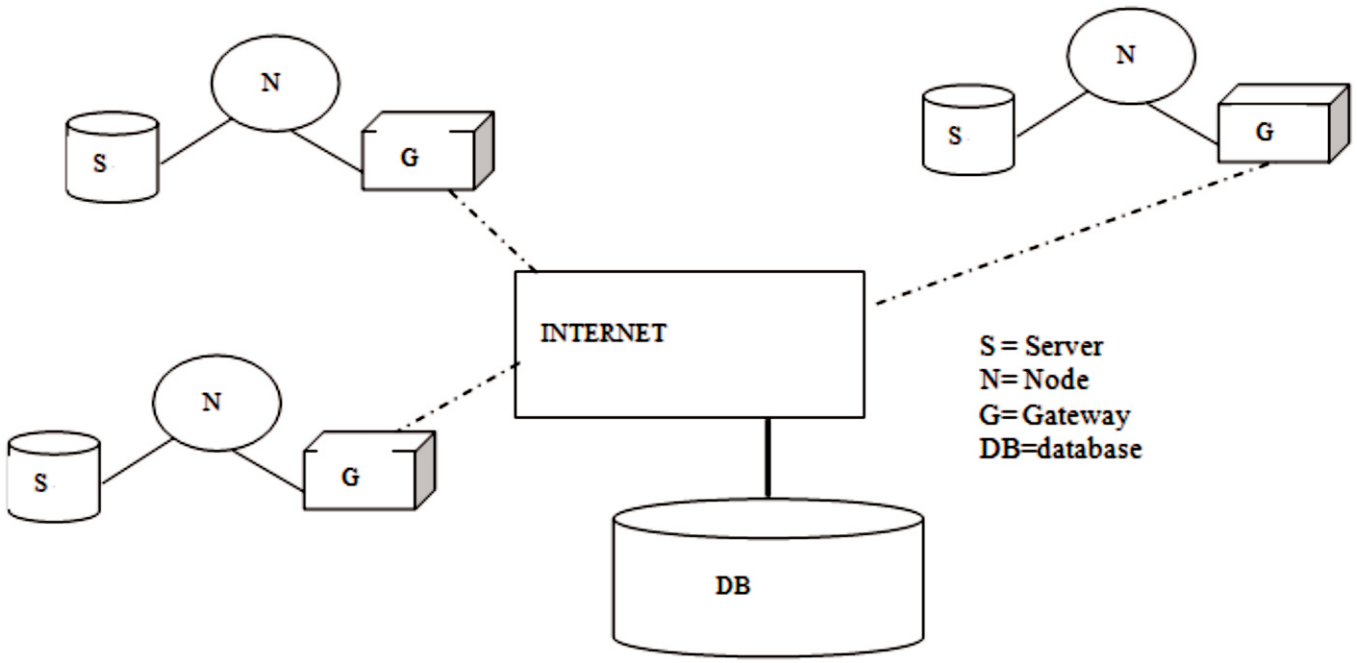

Figure 1. Sensor Networks Radically Expand the Existing Internet into Physical Spaces

from TCP are Congestion control based on decoupling and assisted controls, Bit rate based transmission, coordination among multiple layers. Since adhoc wireless networks having unique characteristics such as extremely defenseless while compared with wired networks as show in Table 1.

2. Types

2.1 Byzantine Attacks

A traded off intermediary node or an arrangement of traded off intermediary node works based on knowledge and conveys attacks, for example, creation of routing loops, directing packets on non finest ways and specifically dropping packets. Byzantine failures are difficult to discover. The networks could appear to work typically in the perspective of the nodes; however it might really be displaying Byzantine activities. Byzantine purposely Insider attacks are identified as Byzantine attacks and protocols which can manage the cost of administration within the sight of byzantine nodes are known as Byzantine flexible protocols. "Byzantine issue" is the term that alludes to the conditions where a couple of imperfect/defiled individuals from the gathering demonstrations in a subjective way and cause a framework fault. This sort of issue was first expressed by Sen et al. (2007)as "Byzantine General Problem" (Carbunar et al., 2004). Certain highlights of byzantine attacks are basic like "selfish" node issue like not sending the gotten information packets, but rather the intension of both are very unique. The point of the self-centered node is to participate in the directing and in the system without spending its own assets while; the point of the byzantine node is to intrude on the correspondence of different nodes in the system, without thinking about its own benefit usage. Because of Byzantine attacks the adhoc systems survivability influenced a mass, the majority of the scientists investigated the impacts as far as throughput, PDR, packet drop rate and aggregate overhead measurements that helps in deciding the system execution (Di Crescenzo et al., 2006). Packet delivery ratio: The proportion between the quantities of packets acknowledged by the receiver to the quantity of packets sent to the receiver. Throughput: The aggregate number of packets effectively conveyed to the receiver in a predetermined moment of time. Packet drop rate: The aggregate number of information packets dropped amid the information transmission process. Total

Network Layer Attacks	Proposed Solutions	Advantages	Disadvantages
Byzantine Attack	Secure Routing Protocol	Centralized node will disseminate information to all other nodes.	Many Parameter Measurements are required to find problem.
Blackhole Attack	Key Distribution Scheme	Check by checking the packets history records	Juicing attack is possible
Warmhole Attack	Redundancy and Time Based Hop	Based on the round trip time	Works on limited bandwidth
Sybil Attack	Testing and Verification	Trust based group forming	Information will be broadcasted among group.
Selective Drooping Attack	Reputation Based Mechanism	Will be deliver based on ACK	Delay of conveyance of message.
Selfish Attack	Credit based Incentive System	Node forwards packet without adding phantom links	Strategy is not much efficient
Resource Utilization attacks (Karthik& Krishnan, 2018)	Secure Efficient Distance Vector Routing	Robust against clumsy attacks	When attackers uses same seq. num and metrics
Information Revelation (Karthik & Saranraj, 2018)	LSDA	Higher precision in flow by De-anonymize the networks.	Sharing of location information
Position Revelation	PBR	Higher precision in flow by De-anonymize the networks.	Requires large computational attempt.
Resource Utilization attacks (Karthik & Krishnan, 2018)	Secure Efficient Distance Vector Routing	Robust against clumsy attacks	When attackers uses same seq. num and metrics

Table 1. Units of Magnetic Induction

Overhead: Ratio of the aggregate of information packets and control packets to the quantity of information packets sent by a moving node. Control Overhead: The most extreme number of bytes of control packets conveyed to the receiver at a point of time.

2.2 Blackhole

In Blackhole attacks the suspicious nodes mutely drop or remove all or few of the received packets all time or some time. Suspicious node can promote themselves as having a valid route to some of famous destinations on network. In (Karthik & Krishnan, 2018; Pereira et al., 2018), a defence against Blackhole attacks was proposed when an attacker would counterfeit its history of contacts along some famous destination and rise to maximum value of delivery likelihood. The "Encounter Ticket (ET)" is planned as confirmation of the encounters of nodes. Though a suspicious node can still fake the contact history along a destination through a one-time tailgate attack, where the suspicious node can collect redundant ETs through tailgating the goal once, after that moving about the data source to intercept data. However, even along the author's method of eliminating the redundant ETs formed within a tiny interval, it might not efficiently work in case of multi-tailgate attack, where the attacker will move in and out of the particular destination's connection range. This method can detect only an attacker during claiming non-existent encounters and cannot handle the dropping of packets in Blackhole attack. In suspicious nodes expand their capability of meeting node at destination so it can interrupt data from other senders. A mechanism of watchdog was proposed to observe the neighbour nodes behaviour and without end to end connection. In this mechanism, to inform the sender the next hop honestly to forward data to other nodes a watchdog with a positive feedback message (PFM) is used. While node A is sending a message to node B, node A will watch the forwarding behaviour of node B in terms of confirmation of the PFM created via other nodes such as node C which received message from node B. It shall then generate a PFM generate a PFM and transfer it to node A saying it the message is forwarded successfully. If node A does not

receive this PFM, then node B shall be registered as malicious until the PFM arrives and trust/reputation system is formed based on this mechanism. In this case, every node would have record of trust value for other to create a direct and indirect reputation. This trust value is consequent and integrated along the probability of meeting destination in order to attain final evaluated forward competency for node (Nasser & Chen,2007; Chuah & Yang, 2009). However a PFM is send via epidemic routing. Thus these add more overhead on network. A technique of securing the delivery history of packet between nodes is proposed. Nodes will detect Blackhole attacks through checking the records. In case of meet between two nodes the exchanged packet numbers are recorded between them and private keys are used to generate a secure node. Near-by nodes can do sense check by checking the packets history records of the other nodes, in order to identify more black hole attacks. Private Key (RK) and public key (PK) pairs are there in each node, along each node having the public keys of other nodes. Though the way pre-loading all keys within the nodes during a network setup phase or by a key distribution scheme would be complicated to apply in WSNs.

2.3 Warmhole

The warmhole attacks plan is the suspicious node trace packets in the particular location in network and then tunnel it to the location in the network and again retransmit them from that particular location. In order to attract other nodes or traffic the malicious nodes aver a diminutive path in network. To limit the allowance of maximum transmitting distance few information can be added to packets. By means of receiver of the packet idyllically inside a particular distance from the sender in geographical leaches the temporal and geographical leashes can be used. In order to have upper bound on its life span in the temporal leashes so that it could restrict the maximum travelling distance. Though this technique require secure rigid time synchronization. A technique for detection and isolation of warmhole attacks were proposed in. This is an alteration of the AODV protocol in which the source node drives a request on route to destination and obtains all available routes along the number of hops. These routes are then used after as reference for each other in order to discover the suspicious node. The anticipated method works in three steps through the route redundancy, routes aggregation and calculation of tound-trip time(RTT) for all listed routes(Zhang et al., 2008; Trifunovic et al., 2010; Samara et al., 2020; BenSaleh et al., 2020; Kaur & Kumar,2020). To facilitate the detection of malicious node and then separate it we must do a comparison between RTT and the number of hops for all routes. Although this method will be useful in WSNs since there is no end to end connection and it is hard to identify route more than one to destination.

2.4 Sybil

A Sybil attack is ability of suspicious node to form number of fake ID's during dropping received packets. In Sybil attack it is hard to detect the real node that causes the packet dropping because the suspicious node use different ID's to communicate with near-by. In the taxonomy and definition is proposed for Sybil attacks, showing different type of defence like resource testing which is an old technique and radio resource testing, verification of key sets for random key pre-distribution, registration, position verification, code attestation which is a new technique. Another defence against sybil attack is proposed in by designing a reputation based system such as Implicit and Explicit social trust establishment. This trust relies on twp factors they are first is contact quality within the nodes and trustworthiness of nodes opinions. To establish the social trust the nodes must merge implicit and explicit social trust in which the explicit social trust is created from Friend ties whenever through secure pairing they meet. A friend list is created in every meet and they are saved in friendship graph. Implicit social trust is created from contact time and relies in similarity and familiarity of nodes. Similarity is the degree of familiarity for two nodes matches and familiarity is the accumulation contact time (Li& Das, 2013; De Fuentes et al., 2014).

2.5 Selective Dropping

In usual operation of network according to predefined

rules packets can be dropped. The rules such as resource limitation in which a packet dropping policy, dropping mechanism and performance analysis is projected according to weight of packets. These weights are calculated depending on inter-contact time within the nodes. However, in selective dropping attacks or dropping attacks, suspicious nodes drop some or all of the received packets. It is hard to identify attacker as both source and destination doesn't know where or when the dropping would occur and also since suspicious node is part of network domain. Mechanism based on acknowledgement can be used for identifying attacks of detecting packet. This is based on authenticated acknowledgment from intermediate nodes and destination with particular time period. Source or destination can detect suspicious node. Ina alleviation scheme to calculate the packet selective dropping attack impact is proposed through usage of network coding. In this scheme, the final node should calculate the ratio of delivery and send it back to sender (Ke et al., 2010). The sender dynamically starts adjusting the redundancy factor to alleviate against reduction in delivery ratio due to attacks. Theoretical analysis and simulation describes the impact of dropping packet on performance routing. The impact of action such as selfishness or message non-forwarding in routing performance would reduce the delivery cost, during the behaviour of increase in delivery cost by dropping messages. The work (Kumar & Parimala, 2016) is proposed mechanism for identifying the packet dropping attacks from where in-between nodes acknowledge the reception of packets. Source nodes make use of this acknowledgement to make a Merkle Tree and then compare it with tree root of predefined values. If those values are equal then packet dropping doesn't occur in that path or else the dropping occurs. However, this method would detect the path with suspicious node and look for other path for retransmission. Thus this method would lead in network overhead. This method also cannot identify the accurate suspicious node in the path. In authors proposed a mechanism of packet dropping depending on cooperative participation in network-bootstrapping phase. Another routing is used to avoid non-trusted or suspicious node. However, this result leads to overhead of network. In author has proposed the discovery mechanism for dropping packet attacks depending on the data on data attribution to identify suspicious nodes. The characteristic is exploited to obtain goal. Three stages are there for this technique: direction of lost packets using the distribution of the inter packet delays, identification of the presence of attacks through comparing the empirical average packet loss rate along the rate of natural packet loss of the path of data flow and discover the suspicious path or link and isolate it through transmitting more provenance information along the sensor data. However, this method is not exact since it does not identify the accurate suspicious node in entire link or path. In (Alajeely et al., 2016; Fazlic et al., 2019), two methods were used to pick up throughput pathrater and watch dog. In the watchdog stage a node that sends can identify the misbehaving node through overhearing the neighbour node and compare its transmission message along the saved copy on buffer and ensure whether it's matching. If matched then node is not suspicious and copy of message on buffer is removed. If for a particular time nothing is heard, the watch dog will increase failure tally of nearby node. Each node running the pathrater phase would declare the best path with highest metric through combining information from watchdog with reliability data link, and then calculate the best path. According to information by watchdog and pathrather every node will develop a table on rating for other nodes known on network sp it will be used in further transmissions (Qin& Huang,2011; Baadache & Belmehdi, 2012). However, the watchdog method is not efficient if ambiguous collusion, limited power transmission, receiver collision, false misbehaviour or collusion. To resolve the weakness of watchdog, Exwatchdog was proposed into improve the intrusion de-tecting system to identify suspicious node. Exwatchdog has ability to identify malicious node which partitions the network through falsely reporting other nodes as suspicious. Each node develops a table with number of received packets and the forwarded packet numbers. When the report about a

misbehaving node is received by a node, the source of communication sends message to destination to check whether there are equal number of received and forwarded packets. If they are equal the node that reported that the other node id suspicious is actually suspicious and if they are not equal, the report is correct. The authors in proposed reputation based mechanism for identifying attacks of dropping packets. This mechanism uses direct observation and indirect or second hand information to measure the full reputation weight. Nodes can be removed from the network if they have low reputation weight. To provide fault tolerance, historical reputation and Fuzzy logic was used for enhancing the performance. In the algorithm for detection of packet dropping attacks, and to find suspicious node that attempted the attacks. The algorithm identify the attack through usage of indicative field in header section of each packet; the indicative field has 3 sub fields- the identification field, flag field, and offset field. These 3 field are used to identify whether the node receives the complete original number of packets from previous node. In a novel attack and detection mechanism against special type of attacks of packet dropping where suspicious node one or more packets and inject few new packets instead. The novel detection mechanism is very highly accurate and very powerful. It relies simple yet powerful idea, the creation time of each packets. Results show that this mechanism has very high detection and high accuracy rate.

2.6 Selfish

Selfish nodes make use of network services but they reject to co-operate with other nodes. For example, Selfish node will not route or forward message because of limitation of battery life or consumption of resources. Defence against this kind of attack is classified into credit and barter based. In a barter based mechanism is proposed to kindle selfish node to cooperate. This system contains two parts a virtual payment or rewarding scheme part and reputation part. When transmission ranges are same of two nodes they start sending the explanation of their message on buffer. They would then agree on which message will be exchanged, with each messages sent from each side one by one in preference order of primary/secondary message. If one side deceives, the transaction is interrupted directly and worst case would be the delay of one message. After the interaction of every message the nodes would receive score and they gather these scores in order to get their total score at the end. This batter based mechanism in which the nodes are divided into two players namely Crowd player, represents the majority of nodes by Gaming theory (Kumar& Kumar, 2019; Singh et al., 2018). Deviator player that deviates from behavior of normal node which is represented in small node. However, this method relies on assuming the selected subsets of message should be enough to exchange all messages agrees that are not practical. Also the clear picture of network behavior is not available in case a node few or no message than second side. In a Credit-Based Incentive System is proposed. Each nodes receiver/ client pays for delivery of message payment scheme involving two algorithms. First is an algorithm that decides the relay to paid called payment set selection. Second algorithm is that decides how much is to be paid to each selected relay and how much the client should be charged called as payment calculation algorithm. As a result, nodes forward packets without adding phantom links or degrade contact opportunity until the reward is not enough or is the assessment of underlying routing protocol. This method is not stronger since the sender would flood network as he is not involved in payment schema. This type of strategy is not much efficient whether the majority of node have selfish behavior.

3. Passive and Active Attacks

According to cryptography active attack in communication system is one in which the attacker changes the communication. The alter, counterfeiter, redirect or obstruct the messages. Whereas in passive attack in communication system is in which the invader would snoop and read the messages only and are not able to see it but could make or change the messages. Both the active and passive attacks are in contrast with each other. The active attack which targets the system of communication comprises of the man-in-the-middle attack and rewrite attack. Authentication of

Cryptographic would lead to a entirely complete defense against active attacks. System which has several cryptographic methods is also called as hybrid cryptosystems. The powerful passive attacks are of two they are linear cryptanalysis and differential cryptanalysis. Examples of active attacks are impersonating, jamming, denial of service (DoS). Examples of passive attacks are traffic analysis and monitoring and eavesdropping.

4. Cryptography

Cryptography is the word crypto means secret and graphy means writing. This attack is a technique of circumventing of security by means of finding the fault in code, cipher etc. It is concerned with algorithm developing. It is the art or sciences that include principles and technique such as transforming the intelligible message to unintelligible and retransform to original form.

Conclusion

In this survey, the various types of attacks in network has been described and analyzed. We discussed the defence against those attacks. The various examples of particular attacks were taken into consideration. Some sub classifications of attacks were also discussed here. The secure routing techniques in WSNs can be made by using those defence mechanism against various attacks. In summary, some of the examples and defence of that particular attack would lead to have a secured communication in the network. Secured communication is obtained by avoiding the unwanted interrupt in the network.

Reference

[1]. Alajeely, M., Doss, R., & Ahmad, A. A. (2016). *Security and trust in opportunistic networks–A survey.* IETE Technical Review, 33(3), 256-268. https://doi.org/10.1080/02564602.2015.1094383

[2]. Baadache, A., &Belmehdi, A. (2012). Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks. *Journal of Network and Computer Applications,* 35(3), 1130-1139. https://doi.org/10.1016/j.jnca.2011.12.012

[3]. BenSaleh, M. S., Saida, R., Kacem, Y. H., & Abid, M. (2020). Wireless sensor network design methodologies: A survey. *Hindawi Journal of Sensors,* 43(3), 56-69. https://doi.org/10.1155/2020/9592836

[4]. Carbunar, B., Ioannidis, I., & Nita-Rotaru, C. (2004, October). JANUS: towards robust and malicious resilient routing in hybrid wireless networks. In *Proceedings of the 3rd ACM workshop on Wireless security* (pp. 11-20). https://doi.org/10.1145/1023646.1023649

[5]. Chuah, M., & Yang, P. (2009, August). Impact of selective dropping attacks on network coding performance in dtns and a potential mitigation scheme. In 2009, *Proceedings of 18th International Conference on Computer Communications and Networks* (pp. 1-6). IEEE. https://doi.org/10.1109/ICCCN.2009.5235372

[6]. De Fuentes, J. M., González-Manzano, L., González-Tablas, A. I., & Blasco, J. (2014). *Security models in vehicular ad-hoc networks: A survey.* IETE Technical Review, 31(1), 47-64. https://doi.org/10.1080/02564602.2014.890844

[7]. Di Crescenzo, G., Ge, R., & Arce, G. R. (2006). Securing reliable server pooling in MANET against byzantine adversaries. *IEEE Journal on Selected Areas in Communications,* 24(2), 357-369. https://doi.org/10.1109/JSAC.2005.861393

[8]. Doherty, L. (2001). Energy and performance considerations for smart dust. *International Journal of Parallel Distributed Systems and Networks,* 4(3), 121-133.

[9]. Fazlic, F., Hashemi, S. A., Aletic, A., Abd Almisreb, A., Norzeli, S. M., & Din, N. M. (2019). A Survey On Security In Wireless Sensor Network. *Southeast Europe Journal of Soft Computing,* 8(1), 35-41. https://doi.org/10.21533/scjournal.v8i1.174

[10]. Karthik, R., & Krishnan, M. N. (2018). Implementation of smart irrigation system for preserving the growth of crops. *International Journal of Modern Trends in Engineering and Science.* 5(3), 29-32.

[11]. Karthik, R., & Saranraj, B. (2018). Dual optimization solution towards achieving a energy efficiency and fault tolerance through mobile sinks on cluster based wireless sensor network. *Journal of Advance Research in Dynamical & Control Systems,* 10(10).

[12]. Kaur, T., & Kumar, D. (2020). A survey on QoS

mechanisms in WSN for computational intelligence based routing protocols. *Wireless Networks,* 26(4), 2465-2486. https://doi.org/10.1007/s11276-019-01978-9

[13]. Ke, M., Nenghai, Y., & Bin, L. (2010, November). A new packet dropping policy in delay tolerant network. *In 2010, IEEE 12th International Conference on Communication Technology* (pp. 377-380). IEEE. https://doi.org/10.1109/ICCT.2010.5689151

[14]. Kumar, G. D., & Parimala, V. (2016). Optimization of network lifetime using layer determination scheme with node rotation. *Asian Journal of Research in Social Sciences and Humanities,* 6(9), 608-618. https://doi.org/10.5958/2249-7315.2016.00821.2

[15]. Kumar, V., & Kumar, A. (2019). Improving reporting delay and lifetime of a WSN using controlled mobile sinks. *Journal of Ambient Intelligence and Humanized Computing,* 10(4), 1433-1441. https://doi.org/10.1007/s12652-018-0901-5

[16]. Lamport, L., Shostak, R., & Pease, M. (2019). The Byzantine generals problem. In Concurrency: the Works of Leslie Lamport (pp. 203-226). https://doi.org/10.1145/3335772.3335936

[17]. Li, N., & Das, S. K. (2013). A trust-based framework for data forwarding in opportunistic networks. *Ad Hoc Networks,* 11(4), 1497-1509. https://doi.org/10.1016/j.adhoc.2011.01.018

[18]. Liu, J., & Singh, S. (1999, September). ATP: application controlled transport protocol for mobile ad hoc networks. In *WCNC. 1999 IEEE Wireless Communications and Networking Conference* (Cat. No. 99TH8466) (Vol. 3, pp. 1318-1322). IEEE. https://doi.org/10.1109/WCNC.1999.796951

[19]. Liu, J., & Singh, S. (2001). ATCP: TCP for mobile ad hoc networks. *IEEE Journal on Selected Areas in Communications,* 19(7), 1300-1315. https://doi.org/10.1109/49.932698

[20]. Nasser, N., & Chen, Y. (2007, June). Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc networks. In 2007, *IEEE International Conference on Communications* (pp. 1154-1159). IEEE. https://doi.org/10.1109/ICC.2007.196

[21]. Pereira, F., Correia, R., & Carvalho, N. B. (2018, June). Comparison of active and passive sensors for IoT applications. In 2018, *IEEE Wireless Power Transfer Conference (WPTC)* (pp. 1-3). IEEE. https://doi.org/10.1109/WPT.2018.8639445

[22]. Qin, Y., & Huang, D. (2011, June). Least squares disclosure attack in mobile ad hoc networks. In 2011, *IEEE International Conference on Communications (ICC)* (pp. 1-5). IEEE. https://doi.org/10.1109/icc.2011.5962524

[23]. Samara, G., Besani, G. A., Alauthman, M., & Khaldy, M. A. (2020). Energy-Efficiency routing algorithms in wireless sensor networks: A Survey. *International Journal of Scientific & Technology Research,* 9(1), 271-283.

[24]. Sen, J., Chandra, M. G., Balamuralidhar, P., Harihara, S. G., & Reddy, H. (2007, May). A distributed protocol for detection of packet dropping attack in mobile ad hoc networks. In 2007, *IEEE International Conference on Telecommunications and Malaysia International Conference on Communications* (pp. 75-80). IEEE. https://doi.org/10.1109/ICTMICC.2007.4448606

[25]. Singh, M. K., Amin, S. I., Imam, S. A., Sachan, V. K., & Choudhary, A. (2018, October). A survey of wireless sensor network and its types. In 2018, *International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)* (pp. 326-330). IEEE. https://doi.org/10.1109/ICACCCN.2018.8748710

[26]. Trifunovic, S., Legendre, F., & Anastasiades, C. (2010, March). Social trust in opportunistic networks. In 2010, *INFOCOM IEEE Conference on Computer Communications Workshops* (pp. 1-6). IEEE. https://doi.org/10.1109/INFCOMW.2010.5466696

[27]. Zhang, X., Jain, A., & Perrig, A. (2008, December). Packet-dropping adversary identification for data plane security. In *Proceedings of the 2008 ACM CoNEXT Conference* (pp. 1-12). https://doi.org/10.1145/1544012.1544036

ABOUT THE AUTHORS

K. Thamizhmaran has received his M.E, M.Sc (yoga) degree from Annamalai University, Tamilnadu, India in the year of 2012 & 2018 respectively. He is pursuing Ph.D (networking) & PG diploma guidance and counseling from Annamalai University, He is currently working as an Assistant Professor in ECE, Department of Electronics and Communication Engineering, Government College of Engineering, Bodinayakkanur, Theni, Tamilnadu, India. He is a Reviewer of 11 International Journals. His research interested includes Networks security, Ad-hoc Networks, Mobile Communications. He has published more than 121 technical papers at various National / International Conferences and Journals. He is a member of 13 Professional bodies.