International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 5 | ISSN : 2456-3307

# Identification of Dropout Packets in Wireless Sensor Networks

**S. Thiruvengadam*[1], Dr. K. Thamodaran[2]**

*[1]MPhil Research Scholar, Department of Computer Science, Maruthupandiyar College, Thanjavur, Tamilnadu, India
[2]Professor, Department of Computer Science, Marudupandiyar College, Thanjavur, Tamilnadu, India

## ABSTRACT

The wireless networks formulate significant revolution in the field of information and communications technology. The wireless networks connect multiple computers and communications devices mutually devoid of wires. The security of data is very important issue in any kind of wireless networks. Wireless sensor network and its applications by intrusions and other attacks to interrupt the characteristics it serves. Normally packet loss is occurring by network congestion. Packet loss is measured as a percentage of packets lost with respect to packets sent. Network congestion in data networking is reducing the quality of service that occurs when a network node is carrying more data than it can handle. In this paper, a network security framework is developed to detect the packet loss and the nodes are offering statement about packet losses. This framework is also offering the features for improving the detection accuracy, and identification of correlations between lost packets. This technique affords privacy preserving, collusion proof, and incurs low communication and storage overheads.

**Keywords:** Detection Accuracy, Network Congestion, Packet Losses, Security, Wireless Networks.

## I. INTRODUCTION

Computer or communication networks can be generally classified based on whether they are physically connected or are intermittently connected using radio signals. Computer networks that are connected by a piece of wiring, such as a coaxial cable are known as *wired networks*. Wireless networks use *radio signals* as their physical layer. The ability to connect two or more computers without the need of cumbersome wiring and the flexibility to adapt to mobile environments have been fueling the widespread acceptance and popularity of wireless networks [8]. A Wireless Sensor Network is a combination of wireless networking and embedded system technology that monitors physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. Initially, Wireless Sensor Networks were mainly used for military surveillance [2], [6].

Wireless communications have happen to a very attractive and interesting region for the provision of electronic services. Mobile networks are available almost anytime and anywhere, and the popularity of wireless handheld devices is high. The services offered are strongly increasing because of the wide range of the users' needs. They vary from simple communication services to applications for special and sensitive purposes such as electronic commerce and digital cash. As wireless devices are used in offices and houses, the need for strong and secure transport protocols seems to be one of the most important issues in mobile standards. It is apparent that wireless protocols and communication networks security will play a vital role in transmitted information operations. From e-mail services to cellular-provided applications and from secure internet possibilities to banking operations, cryptography is an essential part of today's users' needs. Recent and future mobile communication systems have special needs for cryptography [10].

Information and Communication Technologies (ICT) security considers the security of information from a technological perspective, while information security is a wider concept that considers all aspects of information, independently of the medium, as well as the handling of information. The concept of information security includes all the disciplines related to ICT security, such as network security, application security, physical security and logical security, as well

as the business view. Information security is contains three kinds of components such as i) Information security requirements, representing the security goals, (ii) Information security policy, representing the steps to be undertaken in order to ensure an adequate level of security protection, (iii) Information security mechanism, representing the technical tools, operational tools and managerial tools to be used in order to enforce the policy [14].

Network security is the process by which digital information assets are protected, the goals of security are to protect *confidentiality*, maintain *integrity*, and assure *availability*. The MAC address is unique number, which cannot be changed. The list of IP address used in network and then bind those IP addresses to the particular systems MAC address. After doing this activity no one can use system or laptop in this system. Network security involves the authorization of access to data in a network, which is controlled by the network administrator [3].

In order to achieve secure communication in wireless sensor networks the secret keys should be used to encrypt wireless communication and establish data *confidentiality, integrity* and *authentication* among sensor nodes. Therefore, it is necessary to develop appropriate security mechanism for wireless sensor network to distribute secret keys into sensors, encrypt wireless communication and establish authentication among sensor nodes. In this paper, an analytical framework based on forensic analyzer is proposed to distinguish the packet loss with likelihood of a transmitter or receiver discarding packets maliciously with high accuracy.

The organization of this paper is as follows. In Section II the related work is presented, section III explain about Methods and Materials that includes wireless networks, secure data aggregation, network congestion and packet loss, transmission evidence, section IV offers the proposed security framework, experimental results and discussion is illustrated in section V and section VI finish off this paper.

## II. RELATED WORK

The several existing works related to the proposed Wireless Networks security system "Identification of Dropout Packets in Wireless Sensor Networks" are presented in this section. Wireless is a broad term that encompasses all sorts of technologies and devices that transmit data over the air rather than over wires, including cellular communications, networking between computers with wireless adapters and wireless computer accessories. In an ad hoc network in the presence of nodes that throughput in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so [15],[21].

S. Marti, T. J. Giuli, K. Lai, and M. Baker presented the system to categorize the nodes based upon their dynamically measured behavior. In this system *watchdog* is used to identify the misbehaving nodes and a *pathrater* that helps routing protocols avoids these nodes. With help of simulation evaluate watchdog and pathrater using packet throughput, percentage of overhead (routing) transmissions, and the accuracy of misbehaving node detection. When used together in a network with moderate mobility, the two techniques increase throughput by 17% in the presence of 40% misbehaving nodes, while increasing the percentage of overhead transmissions from the standard routing protocol's 9% to 17%. During extreme mobility, watchdog and path rater can increase network throughput by 27%, while increasing the overhead transmissions from the standard routing protocol's 12% to 24% [1].

Starsky H.Y. Wong, Hao Yang, Songwu Lu and Vaduvur Bharghavan have recommended the Rate adaptation mechanism unspecified by the 802.11 standards, yet critical to the system performance by exploiting the multi-rate capability at the physical layer. This mechanism is used to conduct a systematic and experimental study on rate adaptation over 802.11 wireless networks. Consequently, the new Robust Rate Adaptation Algorithm (RRAA) that addresses the above challenge. RRAA uses short-term loss ratio to opportunistically guide its rate change decisions, and an adaptive RTS filter to prevent collision losses from triggering rate decrease. The experiments have shown that RRAA outperforms three well-known rate adaptation solutions (ARF, AARF, and Sample Rate) in all tested scenarios, with throughput improvement up to 143% [5].

Lili Qiu, Yin Zhang, Feng Wang, Mi Kyung Han, Ratul Mahajan have designed a general model to estimate the throughput and good put between arbitrary pairs of nodes in the presence of interference from other nodes in a wireless network. This model is designed based on measurements from the underlying network itself and is thus more accurate than abstract

models of RF propagation such as those based on distance. The seed measurements are easy to gather, requiring only O(N) measurements in an N-node networks. Based on simulations and measurements from two different wireless test beds, the predictions of our model are accurate in a wide range of scenarios [9].

S. Yang, S. Vasudevan, and J. Kurose suggested a detection scheme to identify a node that incorrectly forwards packets in a static wireless ad hoc network. This scheme detect a misbehaving node based on observations made by neighboring nodes (witnesses) near the forwarding node and also decides whether a node is correctly forwarding a packet or not instantly. Through extensive analysis under various threat scenarios, this scheme unambiguously identifies a misbehaving node when there is no collusion. This scheme has high detection accuracy and accounting for the lossy nature of wireless links, finding that our scheme can achieve high detection accuracy while incurring low communication overhead [11]. J.Tang, Y. Cheng, Y. Hao, and C. Zhou have presented the scheme for real-time detection of selfish behaviour based on sequential probability in wireless networks. This scheme identifies the back off manipulation or to restrict manipulation such as sending scrambled frames. The sender from being selfish DOMINO can detect other misbehaviors in addition to backoff manipulation such as sending scrambled frames, "using smaller DIFS and using oversized NAV [12].

D. Dong, X. Liao, Y. Liu, C. Shen and X. Wang have conducted a formal study on optimizing network topology for edge-self monitoring in sensor networks with the objective of maximizing the lifetime of the network. The focus is on optimized selection of monitor nodes that monitor communication links to reduce the number of monitor nodes. This study work focuses on reducing the active time of the monitor nodes instead of reducing the number of monitor node. While the overall energy consumption may be reduced, some nodes' energy may be depleted sooner than the rest [13].

S.Shen has suggested game theory based modeling is utilized for intrusion detection in wireless networks [15]. U.Paul, Anand Kashya p, S.R.Das, and R.Maheshwari have suggested a monitoring mechanism for single channel only to solve manipulation of the carrier sense behavior due to normal fluctuations of wireless channel[17]. The wireless monitoring system consists of a set of devices known as sniffers, to observe traffic characteristics on the wireless medium. Wireless monitoring is useful for understanding the traffic characteristics or detecting the anomaly in wireless networks. R. Zheng, T. Le and Z. Han have offered monitoring system. In this system an optimal selection of m out of M sniffers and assignment of each sniffer to one of the K channels to maximize the total amount of information gathered in a multi-channel wireless network is done in [19].

Mohammad Al-Rousan et. al have developed an adaptive security protocol for two-layer clustered heterogeneous wireless sensor networks that can toggle between five different modes of operation, each with different security level. Each level of security has its own encryption or decryption algorithm and specified key length depending on the situation of the application and the situation for the wireless sensor networks [22]. G.Premkumar, C.Vinoth, R. Srinivasan have offered a system to find the misbehaviours systems in the wireless network using the passive monitoring method. This system is used to deploying sniffers to all the channels. The IEEE 802.11 technology support many channels but wireless interference only monitoring one channel at a time. This system needs most accurate samples to produce the best results, using sniffers to deploy in the all the channels. The goal of this system is to monitor the wireless networks to capture the many frames and the sniffers to produce the n number of samples to analysis the network traffic. In that sniffers output apply to the hidden Markov model to analysis and find out the misbehaviour systems in the Wi-Fi [23].

R.Muradore and D. Quaglia have recommended a security scheme for Intrusion Detection. In this scheme packet based selective encryption is used for reducing the energy consumption during intrusion detection for networked control systems security. Reduction of energy consumption by intrusion detection systems is being researched in the context of wired networks too [24]. Manoj Kumar Gupta, Lokesh Singh have offered a security system to Detect Intruder in Hierarchical WSN Network. In this system an interruption discovery strategy has been presented utilizing Min Max K-means clustering algorithm, which defeats the lack of affectability to starting focuses in K-means algorithm, and expands the nature of clustering. The investigates

the NSL-KDD information set demonstrate that the proposed strategy is more effective than that in view of K-means clustering algorithm. Additionally, the strategy has higher discovery rate and lower false positive recognition rate [25].

Priti Kharche et. al have proposed the Assistant Cluster Head (ACH) in each cluster with MAODV protocol system to protect data loss. This system is not providing any data loss prevention measure if cluster head or relay node is compromised by attacker. If the cluster head is caused by attack, then this ACH collect the data from all cluster members and forward it to the base station. Experimental results show that the MAODV protocol with ACH provide better data loss prevention, save energy than the existing LEACH, HEED and MAODV protocol [26]. Waleed Al Shehri have conducted a detailed survey on different security approaches for WSNs, examining various types of attacks and corresponding techniques for tackling these issues. The strengths and weaknesses for each technique are also discussed [27]. Abdelmalek Boudries, M Amad, P Siarry have offered a two-phase restoration algorithm. It searches the redundant nodes using the cluster heads, then restores connectivity, and energy consumption is taken into consideration [28]. Wireless sensor networks (WSNs) are indispensable components of Internet of Things [29], [30].

## III. METHODS AND MATERIAL

### A. Wireless Sensor Networks

Wireless sensor networks consist of too many sensor nodes that are distributed in a field and have physical capabilities to measure or sense things in the real world, do some computations, communicate with each other and deliver intended results to a base station. The Wi-Fi covers technologies that incorporate 802.11 standards, such as 802.11g or 802.11ac network cards and wireless routers. These sensors have limited computation and a limited power as well. Wireless Sensor Networks (WSN) increased various research activities because of the exciting and convincing reasons offered by the potential for important monitoring applications on different subjects.

The main aim of the sensor network is to separate tiny sensing devices that are capable of sensing alterations of incidents or parameters and corresponding with other devices over a particular geographic area for target tracking, surveillance, environmental monitoring etc. The sensor network is a special type of network in which it shares some common properties of typical computer network. The goal of security services in WSN's is to protect network i.e. information and resources from attackers. Wireless Sensors Network authentication is a growing technology resulting from progress of different fields for minimizing the false data attacks.

In Wireless communication system the well-established 20 MHz Radio channel that has been widely used in 802.11 from the first standardization of OFDM in 802.11a and the 40 MHz channel used in 802.11n, the 802.11ac brings two new channel sizes. Just as in previous OFDM-based transmission, 802.11ac divides the channel into OFDM subcarriers, each of which has a bandwidth of 312.5 kHz. Each of the subcarriers is used as an independent transmission, and OFDM distributes the incoming data bits among the subcarriers. A few subcarriers are reserved and are called pilot carriers; they do not carry user data and instead are used to measure the channel. To increase throughput, 802.11ac introduces two new channel widths. All 802.11ac devices are required to support 80 MHz channels, which doubles the size of the spectral channel over 802.11n. It further adds a 160 MHz channel option for even higher speeds. Due to the limitations of finding contiguous 160 MHz spectrum, the standard allows for a 160 MHz channel to be either a single contiguous block or two non-contiguous 80 MHz channels [18].

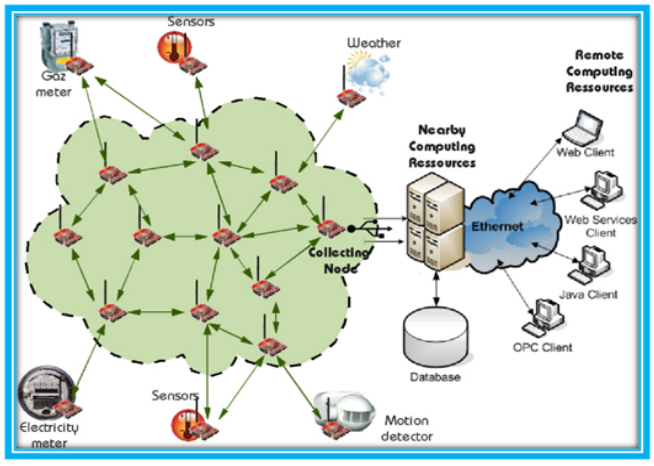


**Figure 1.**Architecture of Wireless Sensor Networks

### B. Secure Data Aggregation

Aggregation is utilized to reduce the quantity of network traffic that helps to reduce energy

consumption on sensor nodes. A wireless sensor network typically consists of a sink node sometimes referred to as a base station and a number of small wireless sensor nodes. The base station is assumed secure with unlimited available energy while the sensor nodes are assumed unsecured with limited available energy. The sensor nodes monitor a geographical area and collect sensory information. Sensory information is communicated to the base station through wireless hop-by-hop transmissions. To conserve energy this information is aggregated at intermediate sensor nodes by applying a suitable aggregation function on the received data. Although complicates the already existing security challenges for wireless sensor networks and requires new security techniques tailored specifically for this scenario. Providing security to aggregate data in wireless sensor networks is known as secure data aggregation in WSN [16], [19], [25].

Two main security challenges in secure data aggregation are *confidentiality a*nd *integrity* of data. While encryption is traditionally used to provide end to end confidentiality in wireless sensor network, the aggregators in a secure data aggregation scenario need to decrypt the encrypted data to perform aggregation. This exposes the plaintext at the aggregators, making the data vulnerable to attacks from an adversary. Similarly an aggregator can inject false data into the aggregate and make the base station accept false data. Thus, while data aggregation improves energy efficiency of a network, it complicates the existing security challenges [4],[7],[20].

### C. Network Congestion and Packet Losses

The service quality of data networking and queuing theory is the reduced due to network congestion that occurs when a network node is carrying more data than it can handle. Typical effects include queuing delay, packet loss or the blocking of new connections. A consequence of congestion is that an incremental increase in offered load leads only to either a small increase or even a decrease in network throughput. Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is typically caused by network congestion. Packet loss is measured as a percentage of packets lost with respect to packets sent. When content arrives for a sustained period at a given router or network segment at a rate greater than it is possible to send through, then there is no other option than to drop packets. If a single router or link is constraining the capacity of the complete travel path or of network travel in general is known as a bottleneck.

### D. Hop-Level Transmission Evidence and Path Level Transmission Evidence

1) ***Hop-Level Transmission Evidence (HTE):***

The availability of hop-level TE reflects the likelihood that evidence exists relating to transmissions on a link. In a multi-hop static wireless network, nodes maintain evidence relating to transmissions as follows:

*Step 1.* A sender or transmitter keeps the signed ACK it receives for each packet it sends.

*Step 2.* A receiver creates an entry locally for each unique packet received and digitally verified.

*Step 3.* A monitoring (witness) node creates an entry locally for each packet that it overhears and verifies.

2) ***Path-Level Transmission Evidence (PTE) :***

Subsequently, the path-level TE is the evidence relating to all transmissions on an end-to-end path. The TE availability on each hop along the path is assumes independent of that on the other hops. Again, in reality the TE availability across hops may be correlated. This idea is utilized for tractability; the simulations and experiments verify that this assumption is indeed acceptable.

## IV. PROPOSED SYSTEM

### A. Media Access Control (MAC) Protocols

In IEEE 802 reference model of computer networking, the medium access control or Media Access Control (MAC) layer is the lower sub layer of the data link layer (layer 2) of the seven-layer ISO OSI model. The MAC sub layer provides addressing and channel access control mechanisms that make it possible for several terminals or network nodes to communicate within a multiple access network that incorporates a shared medium, e.g. an Ethernet network. The hardware that implements the MAC is referred to as a media access controller. The MAC sub layer acts as an interface between the logical link control (LLC) sub layer and the network's physical layer. The MAC layer emulates a full-duplex logical communication channel in a multi-

point network. This channel may provide unicast, multicast or broadcast communication service.

This channel access control mechanisms provided by the MAC layer are also known as a multiple access protocol. This makes it possible for several stations connected to the same physical medium to share it. Examples of shared physical media are bus networks, ring networks, hub networks, wireless networks and half-duplex point-to-point links. The multiple access protocol may detect or avoid data packet collisions if a packet mode contention based channel access method is used, or reserve resources to establish a logical channel if a circuit-switched or channelization-based channel access method is used. The channel access control mechanism relies on a physical layer multiplex scheme.

### B. Hash Key Authentication

The cryptographic hash function is playing vital role in mapping data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hash codes, hash sums, or simply hashes. One use is a data structure called a hash table, widely used computer software for rapid data lookup. Hash functions accelerate table or database lookup by detecting duplicated records in a large file. They are also useful in cryptography. A cryptographic hash function allows one to easily verify that some input data maps to a given hash value, but if the input data is unknown; it is deliberately difficult to reconstruct it (or equivalent alternatives) by knowing the stored hash value. This is used for assuring integrity of transmitted data, and is the building block for HMACs, which provide message authentication.

### C. Proposed Algorithm for Pocket Loss Identification

In the proposed forensic analysis of packet losses, analytical framework facilitates the estimation of the likelihood of either a transmitter and or a receiver discarding packets, given the conditions in the network. The framework is used as the basis for a protocol within a forensic analyzer. It takes the following as input

i). The network parameters,

ii). Monitoring logs for the considered link; it then yields the likelihood that the transmitter or the receiver on the link has discarded packets.

#### 1) *Algorithm for Detection of Packet Losses in WSN*

*Step 1.* Initialize the packet transmission process.
*Step 2.* Choose the source and destination nodes for transmission process.
*Step 3.* For Each packet transfer check the size of queue if size of queue <= Max size then send.
*Step 4.* Checking the node status. If critical situation occurs in the network environment then perform detection phase.
*Step 5.* Stop the packet transmission process and detect the fake node.

An extensive simulations and comparison are conducted and assess the results with ground truth. It is proved that this analyzer facilitates assessments with high accuracy; in particular, they deviate from the ground truth by 2.3%, on average. The cooperative game theory can be used to model situations in which players coordinate their strategies and share the payoffs between them. The output of the game must be in equilibrium so that no player has incentive to break away from the coalition. The game setting in all the earlier game-theoretic work on IDS involves two sets of opposing players, the nodes/IDSs and the attacker or defaulters. In this system, game is established which involves players (IDSs sitting in neighbouring nodes) cooperating to achieve a common goal (i.e., to monitor a single node). The cooperative multi-player game to model the interactions between the IDSs in a neighbourhood and used it to validate our proposed probabilistic scheme is presented.

#### 2) *Progress of Proposed Framework*

i) An innovative technique based on a probabilistic model, to optimize the active time duration of intrusion detection systems (IDSs) in a MANET. The scheme reduces the IDSs' active time as much as possible without compromising on its effectiveness.
ii) In order to validate our proposed approach, present a multi-player cooperative game that analyzes the effects of individual intrusion detection systems with reduced activity on the network.

iii) During simulation, proved that a considerable saving in energy and computational cost is achieved using our proposed technique of optimizing the active time of the IDSs while maintaining the performance of the IDS.

iv) The proposed scheme uses local information, thus making it distributed and scalable. Moreover, it works on both static and mobile networks.

**3) Merits of Proposed Framework**

This proposed framework contains the following merits.

i) Reduce the impact of false recommendation.

ii) High accuracy of trust value.

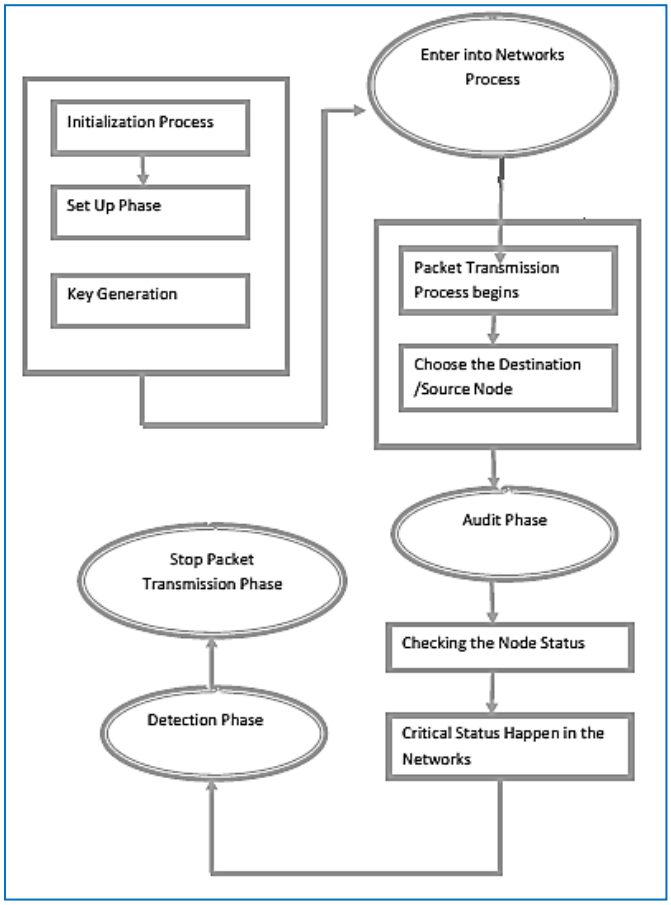


**Figure 2.**Architecture of Security Framework to Detect pocket losses in WSN

### D. Message Authentication Code Algorithm

Message authentication code consists of three algorithms:

*Step 1.* The key generation algorithm selects a key from the key space uniformly at random.

*Step 2.* The signing algorithm efficiently returns a tag given the key and the message. .

*Step 3.* The verifying algorithm efficiently verifies the authenticity of the message given the key and the tag.

For a secure unforgeable message authentication code, it should be computationally infeasible to compute a valid tag of the given message without knowledge of the key, even if for the worst case then assume the adversary can forge the tag of any message except the given one.

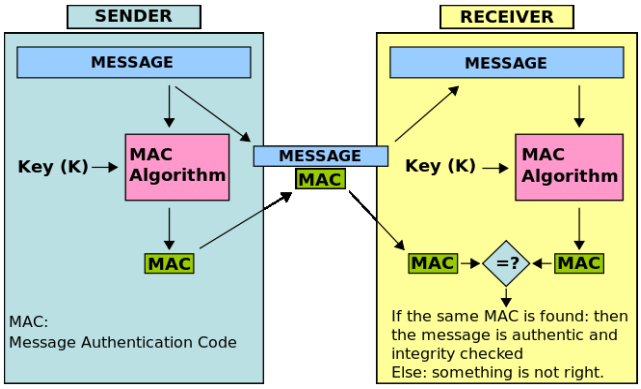


**Figure 3.** Message Authentication Code Algorithm

## V. RESULTS AND DISCUSSION

In the proposed framework the forensic analyzer computes offline, the probabilities of packet losses and TE availability under different conditions, in a benign setting on a link, based on a set of network parameters. It then compares these computed values with what is observed during network operations to estimate the likelihood of a transmitter or receiver discarding packets and lying about the same.

The following functions are performed.

i). Message Authentication Code

ii). Hash Key Function

iii). Multi-factor Authentication

iv). Alert Correlation

TABLE I. THE RESULTS OF VARIOUS FUNCTIONS OF PROPOSED SYSTEM

| Process | Message Authentication | Hash Key Function | Alert Correlation |
|---|---|---|---|
| Node Login | 4.3 | 2.4 | 5.0 |
| Packet Transmission | 2.5 | 4.4 | 3.6 |
| Fake Appearance | 3.5 | 1.8 | 4.5 |
| Alarm Generated | 4.5 | 2.8 | 5.0 |

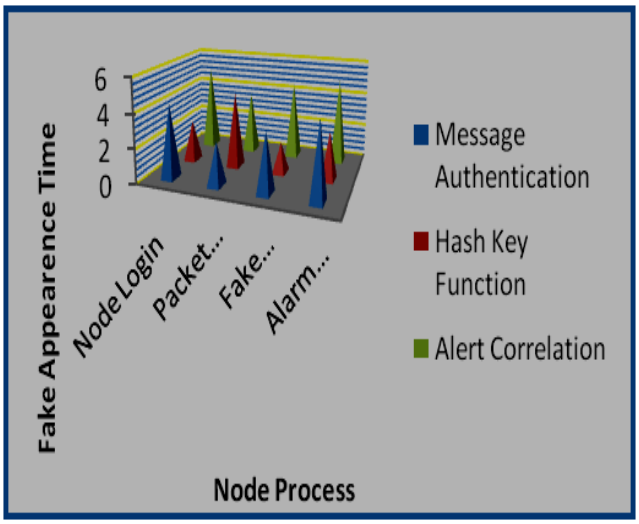


**Figure 4.**The Process of Packet Transmission in Wireless Network

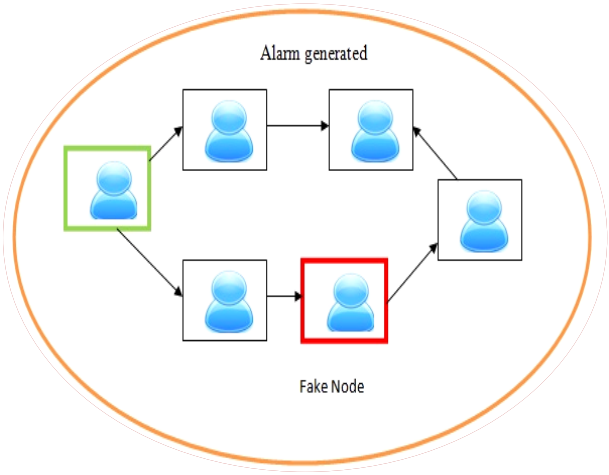


**Figure 5.** Identification of Fake Node

When a critical event occurs, an alarm message should be broadcast to the entire network as soon as possible. To prolong the network lifetime, some sleep scheduling methods are always employed in WSNs, resulting in significant broadcasting delay, especially in large scale WSNs. In this proposed system a novel sleep scheduling method is utilized to reduce the delay of alarm broadcasting from any sensor node in WSNs. Specifically, two determined traffic paths are designed for the transmission of alarm message, and level-by-level offset based wake up pattern according to the paths, respectively. When a critical event occurs, an alarm is quickly transmitted along one of the traffic paths to a centre node, and then it is immediately broadcast by the centre node along another path without collision.

### A. ANALYSIS

The proposed mechanism is based on detecting the correlations between the lost packets over each hop of the path. The basic idea is to model the packet loss process of a hop as a random process alternating between 0 (loss) and 1 (no loss). Specifically, consider that a sequence of M packets that are transmitted consecutively over a wireless channel. Under different packet dropping conditions, packet loss is identified. The wireless channel is modelled of each hop along PSD (Path to Source and Destination) as a random process that alternates between good and bad states. Packets transmitted during the good state are successful, and packets transmitted during the bad state are lost. It is assumed quasi-static networks, whereby the path PSD remains unchanged for a relatively long time. Detecting malicious packet drops may not be a concern for highly mobile networks, because the fast-changing topology of such networks makes route disruption the dominant cause for packet losses. In this case, maintaining stable connectivity between nodes is a greater concern than detecting malicious nodes. A sequence of M packets is transmitted consecutively over the channel.

TABLE II
THE EFFECTIVENESS OF THE PROPOSED SYSTEM

| Method | Proposed System |
|---|---|
| Message Authentication Code | Able to Monitoring each and every node |
| Hash Key Function | Each Node have separate Keys |
| Multi Factor Authentication | Able to check the node process |
| Alert Correlation | Fake Intimation Process |

## VI. CONCLUSION

An efficient way of using intrusion detection systems (IDSs) that assembles on every node of a mobile ad hoc network (MANET). Primarily present the minimization of the active duration of the IDSs in the nodes of a MANET as an optimization problem. Then the described a cooperative game model to represent the interactions between the IDSs in a neighbourhood of nodes. The game is defined in such a way that the primary goal of the IDSs is to monitor the nodes in its neighbourhood at a desired security level so as to detect

any anomalous behaviour, whereas, the secondary goal of the IDSs is to conserve as much energy possible. In order to achieve these goals, each of the nodes has to participate cooperatively in monitoring its neighbour nodes with a minimum probability. Then a distributed scheme is developed to determine the ideal probability with which each node has to remain active (or switched on) so that all the nodes of the network are monitored with a desired security level.

The evaluation of the proposed scheme is done by comparing the performances of the IDSs under two scenarios: (i) Keeping IDSs running throughout the simulation time and (ii) Using this proposed scheme to reduce the IDS's active time at each node in the network. The simulation results indicates that the effectiveness of the IDSs in the network is not compromised while using the proposed scheme, rather, there is considerable reduction of energy consumption in each of the nodes that increases the network lifetime significantly. The observed results show homogeneous network in a way that all the nodes have the same capacities in terms of their computational and energy resources. In future, the proposed model may extended in heterogeneous network.

## VII. REFERENCES


[1] Marti.S., T. J. Giuli, K. La and M. Baker, "Mitigating Routing Misbehavior in a Mobile Ad-hoc Environment", Proc. 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 255- 265, August 2000.

[2] Mayank .S "Security in Wireless Sensor Networks," In ACM SenSys, 2004.

[3] Simmonds, A; Sandilands, P; van Ekert, L, "An Ontology for Network Security Attacks". Lecture Notes in Computer Science, 3285- pp 317 -323, 2004.

[4] Alpcan.T and T. Basar, "A Game Theoretic Approach to Decision and Analysis in Network Intrusion Detection," Proc. 43rd IEEE Conference on Decision and Control, December 2004.

[5] Starsky.H.Y. Wong, Hao Yang, Songwu Lu and VaduvurBharghavan, "Robust Rate Adaptation for 802.11 Wireless Networks", pp146-147, 2006.

[6] F. Anjum and P. Mouchtaris "Security for Wireless AD HOC Networks" Wiley, 2007.

[7] Hoang.T. Hai and E-N.Huh, "Optimal Selection and Activation of Intrusion Detection Agents for Wireless Sensor Networks", Proc. Future Generation Communication and Networking, vol.1, no., pp.350-355, Dec. 2007.

[8] JagannathanSarangapani, "Wireless Ad Hocand Sensor Networks Protocols, Performance, and Control", CRC Press-Taylor & Francis, 2007

[9] LiliQiu, Yin Zhang, Feng Wang, Mi Kyung Han, RatulMahajan, "A General Model of Wireless Interference", 2007.

[10] Nicolas Sklavos and Xinmiao Zhang, "Wireless Security and Cryptography : Specifications and Implementations", CRC Press-Taylor & Francis, 2007.

[11] Yang.S.,S.Vasudevan, and J. Kurose, "Witness-based detection of forwarding misbehaviors in wireless networks", in UMass Computer Science Technical Report UM-CS-2009-001, 2009.

[12] J.Tang, Y. Cheng, Y. Hao, and C. Zhou, "Real-Time Detection of Selfish Behavior in IEEE 802.11 Wireless Net works," Proc. IEEE 72nd Vehicular Technology Conf. Fall (VTC-Fall), 2010.

[13] D. Dong, X. Liao, Y. Liu, C. Shen and X. Wang, "Edge Self-Monitoring for Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems," vol. 22, no. 3, March 2011, pp. 514-527.

[14] IgliTashi and SolangeGhernaouti-Helie, "Information Security Evaluation-A Holistic Approach", EPFL Press, 2011.

[15] Shen.S., "A game-theoretic approach for optimizing intrusion detection strategy in WSNs", Proc. International Conference on Artificial Intelligence, Management Science and Electronic Commerce, pp.4510-4513, Aug. 2011.

[16] Zeadally.S , R. Hunt, Y-S. Chen, A. Irwin and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges", Telecommunication Systems, vol. 50, no. 4, pp. 217-241, 2012.

[17] U.Paul, AnandKashya p, S.R.Das, and R.Maheshwari, "Passive Measurement of Interference in WiFi Networks with Application in Misbehavior Detection", IEEE Transcations on mobile computing Vol 12,No 3.March 2013.

[18] Matthew S. Gast, " 802.11ac: A Survival Guide", O'Reilly Publishers, August 2013.

[19] Zheng.R., T. Le and Z. Han, "Approximate Online Learning Algorithms for Optimal Monitoring in Multi-Channel Wireless Networks", IEEE Transactions on Wireless Communications, vol.13, no.2, pp.1023-1033, February 2014.

[20] Bhoi.S.K. and P. M. Khilar, "Vehicular communication: a survey", IET Networks, vol. 3, no. 3, pp. 204 - 217, 2014.

[21] Tsikoudis.N, A. Papadogiannakis and E. P. Markatos, "LEoNIDS: a Low-latency and Energy-efficient Network-level Intrusion Detection System," IEEE Transactions on Emerging Topics in Computing, Vol. no. 99, PP142-155, 2014.

[22] Mohammad Al-Rousan, MuneerBaniYassein, Ahmed Al-Dubai, BarraqGhaleb, Ibrahim Mahmoud, A Novel Situation Specific Network Security for Wireless Sensor Networks, Sensors & Transducers, Vol. 186, Issue 3, pp. 33-42, March 2015.

[23] G.Premkumar, C.Vinoth, R. Srinivasan, "Detecting MAC Layer Misbehavior in Wi-Fi Networks by Co-ordinated Sampling of Network Monitoring", International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 5, pp3772-3778, May 2015.

[24] R.Muradore and D. Quaglia, "Energy-Efficient Intrusion Detection and Mitigation for Networked Control Systems Security," IEEE Transactions on Industrial Informatics, Vol. 11, no. 3, pp. 830-840, 2015.

[25] Manoj Kumar Gupta, Lokesh Singh , A Novel Approach to Detect Intruder for Hierarchical WSN Network, International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 2, pp88-92, February 2016.

[26] PritiKharcheet. al, International Journal for Innovative Research in Science and Technology, Volume 2, Issue 11, pp 71-75, April 2016.

[27] Waleed Al Shehri, A Survey on Security in Wireless Sensor Networks, International Journal of Network Security & Its Applications Vol.9, No.1, pp 25-32, January 2017.

[28] A Boudries, M Amad, P Siarry, Novel approach for replacement of a failure node in wireless sensor network.Telecommun Syst. 65, pp 341–350, 2017.

[29] J Li, S Cheng, Z Cai, J Yu, C Wang, Y Li, Approximate holistic aggregation in wireless sensor networks.ACM Trans. Sensor Netw.13(2), Article 11, pp 1–24, 2017.

[30] T Qiu, N Chen, K Li, D Qiao, Z Fu, Heterogeneous ad hoc networks: Architectures, advances and challenges. Ad Hoc Netw.55, pp143–152 , 2017.

## AUTHOR PROFILE

**Mr.S.THIRUVENGADAM** pursed Bachelor of Science from Bharathidasan University, Tamilnadu, India in 2003 and Master of computer applications from the Bharathidasan University, Tamilnadu, India in 2006. He is working as Assistant Professor in Department of Computer Applications at AnjalaiAmmal-Mahalingam Engineering College, Affiliated to Anna University, Chennai. His main research work focus on Computer Networking, Network Security, Big data Analytics, Data Mining, Mobile Computing and Artificial Intelligence. He has 11 years of Teaching Experience and three years of research experience.

**Dr.K.THAMODARAN** pursed Bachelor of Science in year 1988, Master of Science in year 1991 and Master of Philosophy in year 2005 from Bharathidasan University, Trichy, Tamilnadu. He pursed Ph.Din Computer Science from Alagappa University, KaraikudiTamilnadu in year 2014.. He is currently working as Assistant Professor in Department of Computer Science, Marudupandiyar College, Thanjavur, Tamilnadu. He is a life member of ISTE, IAENG and IJCSIT. He has published more than 20 research papers in reputed international journals including Thomson Reuters, UGC Approved journals and conferences including IEEE , Elsevier and it is also available online. His main research work focuses on Network Cryptography, Image Processing, Cloud Security and Privacy, Big Data Analytics and Data Mining. He has 25 years of rich teaching experience and 10 years of Research Experience.