IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

Energy Efficient Encryption Scheme for Integrating Wireless Sensor Networks with Internet

V.Gayathri[1*], Y.S. Kumarswamy[2]

[1]Department of Computer Science., Rayalaseema University, Kurnool, Andra Pradesh, India
[2]Department of Computer Science& Engineering., NCET, Bengaluru, Karnataka, India

[*]*Corresponding Author: vgayathri19@gmail.com,*

DOI: https://doi.org/10.26438/ijcse/v7i3.438448 | Available online at: www.ijcseonline.org

Accepted: 06/Mar/2019, Published: 31/Mar/2019

Abstract- The Internet of Things (IoT) revolution has also impacted Wireless Sensor Networks (WSNs), and due to which, the WSNs are being increasingly coupled with IP network. The security issues which are prevalent in the IP network have to be addressed by these IoT based WSNs. Recently, in the literature, encryption of data packets through 3 Data Encryption Standard (3DES) technique was presented to cater data packet encryption requirements in IoT based WSNs. However, this encryption technique is impractical for WSNs because the sensor nodes operate with limited energy reserves, and 3DES technique is computationally expensive technique. The main open issue is to perform 3DES data packet encryption by incurring limited energy expenditure. To address this open issue, in this paper, a new 3DES data packet encryption scheme denoted as Neighbor Node Cooperation (NNC) scheme is presented. In the NNC scheme, the encryption load of the source node is distributed among its neighbor nodes. Selection of the most suitable neighbor nodes for the NNC scheme is modeled as an optimization problem, which is shown to have non-polynomial complexity. Hence, this optimization problem is approximately solved using randomized algorithm. The formal performance bounds of the randomized algorithm are outlined. The proposed encryption scheme is simulated and compared against the contemporary technique presented in the literature. In the outlined simulation study, the proposed encryption technique significantly outperforms the contemporary technique WRT incurred energy expenditure for data packet encryption.

Keywords—WSN, 3DES, Encryption, IoT

I. INTRODUCTION

The WSNs are essentially used in sensing the required environment using different sensing parameters such as: temperature, humidity, pressure etc. The WSNs are characterized by low cost and low power sensor devices, which have energy resource limitations and perform communication through radio transceivers. The earliest security threats to the WSNs were essentially physical threats; wherein, some of the sensor nodes are modified by the attacker physically, which would result in disastrous consequences to the WSN users. Many security schemes were presented in the literature [1-7] to address the security issues which evolved in classical WSNs. All these presented security schemes ensure that, the cryptographic procedures are energy efficient to prevent fast depletion of node energy reserves; hence, the corresponding encryption schemes of these cryptographic procedures also aim for energy efficiency.

Some of the important issues which create security threats in classical WSNs are outlined below:

1. The sensor nodes usually do not have a fixed structure, because the node locations are randomly selected. Due to the absence of predefined network structure, designing fault tolerance scheme which can operate effectively in all the network structure scenarios is difficult.
2. The link quality between sensor nodes is substantially dependent on the node energy status. If some of the participating nodes in the link become energy depleted, then, the link would become un-operative, and other links may have to be used for data transmission. It must be noted that, some of the links might create relatively more security threats due to the presence of malicious nodes in these links.
3. The sensor nodes have limitations in resources such as: storage capacity, processing capabilities and communication bandwidth. Due to such limitations in resources, utilization of computationally light security mechanisms becomes attractive. However, such computationally light security mechanisms might not be effective in addressing all the major security threats in WSN.
4. Most of the routing protocols which are designed for routing in WSN [8-16], majorly focus on achieving

energy efficiency. However, most of these routing protocols do not consider security issues in their basic design. Hence, security mechanisms have to be built over these routing protocols, which might create a tradeoff between energy efficiency and security effectiveness.

5. Some of the WSNs are deployed in hostile conditions in which, human intervention for regular maintenance of WSNs becomes difficult. In such hostile conditions, the sensor nodes become easy target for physical attack by intruders.

1.1 Addressed Open Issues

The IoT framework has become extremely popular in integrating many physical devices with Internet; so that, these physical devices can be monitored and controlled from any location using IP network. Currently, IoT framework is being extensively used in different domains such as: crime prevention, military, industry, environment, agriculture, infrastructure and urban development [2].

The popularity of IoT framework has also reached the domain of WSNs [8-13]. In-fact, integrating WSN with IoT framework would provide the much needed accessibility advantage to the users, because many WSNs are deployed in hostile conditions, and collecting regular data from such WSNs can require substantial user effort and resources.

The integration of WSNs with IoT framework would create a scenario wherein, the security threats which exclusively plague the IP network, will also start creating security issues in WSNs. Hence, the WSNs have to be enabled to address these exclusive security threats plaguing the IP network. The obvious or straight forward solution to address IP network based security threats in WSNs is to use the established security schemes in the IP network domain which provide effectiveness in addressing such security issues. However, most of these effective security schemes in IP domain are computationally expensive [17], and using such security schemes in WSNs is infeasible due to energy resource limitations in sensor nodes; hence, it would lead to a scenario wherein, tradeoff between energy efficiency and security effectiveness has to be analyzed and incorporated in designing security mechanisms for IoT enabled WSNs; however, in the literature, this tradeoff study has not been effectively performed [17].

One of the popular and effective security schemes in IP network is the 3DES technique [17]. Recently, in the literature [17], the 3DES technique has been utilized to perform encryption of data packets in WSN. However, the encryption scheme presented in [17] does not perform tradeoff analysis study between energy efficiency and security effectiveness, and due to which, the encryption scheme can easily drain node energy reserves and cause network disconnection and also cause severe reduction in network communication effectiveness. Hence, the open issue addressed in this paper is to extend the encryption scheme presented in [17] by achieving the dual goal of improvement in energy efficiency during encryption process and maintaining security effectiveness of the 3DES technique.

In this paper, the 3DES encryption scheme is applied for encryption of WSN data packets in a distributed fashion; wherein, the source node distributes the encryption load to its neighbor nodes. Due to distributed encryption scheme, the source node substantially conserves its energy, and the security effectiveness of the 3DES encryption scheme is maintained. It must be noted that, the proposed distributed 3DES encryption scheme can be directly extended to cater other effective encryption schemes, because the 3DES encryption scheme is only considered as a black box, and the main goal of the proposed scheme is to achieve energy efficiency without sacrificing security effectiveness.

The proposed distributed 3DES encryption scheme is denoted as Neighbor Node Cooperation (NNC) scheme. The NNC scheme is simulated in MATLAB, and compared against the contemporary encryption scheme presented in [17]. In the outlined simulation study, the NNC scheme significantly outperforms the compared scheme in-terms of energy efficiency, and thus, achieves its intended objective of attaining improved energy efficiency and maintaining security effectiveness.

1.2 Paper Contributions

In this paper, the following contributions are made:

1. The NNC scheme is outlined by initially describing the problem formulation. The NNC scheme is modeled through a scoring function to identify the optimal solution for executing it. The non-polynomial complexity of finding the optimal solution of NNC scheme is established. To address the non-polynomial complexity of discovering the optimal solution of NNC scheme, a randomized algorithm is presented. For the proposed randomized algorithm, its: polynomial complexity and probabilistic bounds on the quality of the obtained solution WRT optimal solution are established.
2. The NNC scheme is simulated in MATLAB, and compared with the contemporary technique presented in [17]. The proposed NNC scheme provides substantial merits in-terms of energy efficiency against the contemporary technique. Also, the NNC scheme exhibits noticeable execution efficiency which establishes the feasibility of NNC scheme in being deployed in real world scenarios.

This paper is organized as follows: Section 2 describes the related work corresponding to security techniques in WSN;

Section 3 briefly describes the 3DES technique; the NNC scheme is presented in Section 4; in Section 5, the simulated analysis study of NNC scheme is presented; finally, the paper is concluded in Section 6.

II. RELATED WORK

One of the prevalent attacks in the physical layer is the sweep and reactive jamming attack, which are a kind of DoS attack where the communication channel is jammed. The security mechanism presented in [18] addresses such attacks. Here, secure acknowledgments and channel hopping is employed. However, the threat of wide band jamming is not effectively addressed.

The eavesdropping attack is another popular physical layer attack, where the adversary listens to the communication between nodes through data packet tampering. The security mechanism presented in [19] advocated Message Integrity Code (MIC). However, such measure can lead to increased overheads and transmission delays.

The DoS attack in which data transmission is denied by modifying physical layer and MAC headers, is a special kind of DoS attack. Such kind of DoS attacks were addressed in [18] by suitably encrypting the specific data payload. However, this solution does not cover all the headers, and only covers the MAC header.

The security scheme presented in [20] addressed statistical jamming attack. In this attack, the data packets are subjected to direct attack; since, the adversary has the information about data distribution or protocol details. Here, the proposed solution shortened the size of preamble. However, preamble shortening can limit the performance of MAC protocol.

The denial of sleep attack prevents the node from going into sleep by ensuring that, the node is always active. The solution presented in [21] against such attack, employs multiple counter measures such as: anti reply protection, authentication of link layer, defense against broadcast attack. However, this security scheme has not been effectively tested or simulated.

The fragmentation attack is caused when the packet fragmentation fields are changed, and due to which, reply attacks are inflicted, which results in receiver being flooded by data packets, or even DoS attack might emerge. The security scheme presented in [22] addresses the data fragmentation attack. Here, the security scheme utilized time stamp mechanism to secure against such attacks. However, the formats of legal fragmented packets have not been properly defined, and effective simulation or testing of this security scheme has not been properly done.

Another security scheme for fragmentation attacks is presented in [23]. This scheme utilizes split buffer and content chaining approach. However, significant overheads are created due to this scheme.

The authentication attack is caused when the attacker provides legal authentication for the transmitted data. Such attacks were addressed in [24]; wherein, network access control scheme was utilized to provide node identification. However, this scheme requires substantial testing.

The Botnet attack is caused when the attacker modifies legal data packets, and transmits these tampered packets to the receiving node. Such attacks were addressed in [25], through the design of Bot analysis module. However, this security scheme exhibits significant overheads.

The selective forwarding attack is inflicted when an adversary refuses to route the control or data packets towards intended nodes. The security mechanism presented in [26] -- denoted as Light-weight Heartbeat -- addressed such attacks. However, this security mechanism does not provide any protection after the attack is identified.

Another security mechanism presented in [27] addressed selective forwarding attack, which improved the delivery ratio compared to Light-weight Heartbeat [26]. However, this security mechanism suffers from energy consumption overheads.

The security mechanism presented in [28] addressed the energy consumption overhead issue for the security mechanism presented in [27]; however, it suffers from not providing cent percent true positive rate.

The wormhole attack is inflicted through the creation of low link tunnel in-between two adversary nodes which are situated in different network locations. The Light-weight Heartbeat [26] addressed such attacks; wherein, each network segment was provided with separate keys. However, proper simulation for this security mechanism has not been performed.

The security mechanism presented in [29] also addresses wormhole attack by utilizing Merkel trees authentication. Here, messages are encrypted by nodes through keys. However, until the Merkel tree is established, overheads related to delay and jitter will be created.

The wormhole attack issue was addressed through graph theory approach in [30]. Here, encryption of messages is performed through local broadcast keys. This security mechanism provides the merits of limited overheads and zero synchronization.

The sinkhole attack is created through false information advertisement, which makes the adversary node an attractive center for attracting other sensor nodes. Such attacks will lead to transmission routes being compromised and increased data loss due to reduction in traffic. The security mechanism presented in [31] addresses such attacks by creating necessity for bidirectional communication. Another security mechanism for addressing sinkhole attack was presented in [32]. Here, hybrid mechanisms are utilized, and for dense networks, significant protection against such attacks is provided.

The malicious nodes inflict Sybil attack by creating multiple node identities, which can lead to the compromising of communication routes. The Light-weight Heartbeat [26] also addresses such attacks. However, there are issues regarding node location verification and scaling-up WRT large networks. The security mechanism presented in [33] also addresses Sybil attack. However, it faces the same issues faced by Light-weight Heartbeat [26].

Many routing protocols optimize their performance through operating rules. In the execution of such operating rules, many security threats arise. One such security threat is DAG/DAO inconsistency attack. Here, the malicious node tampers or alters the flags which are used in the identification of network inconsistencies. Due to which, the targeted node will reset trickle timer by discarding the control packet. Hence, more frequent control messages will be transmitted, which creates higher delay and wastage of energy.

The DAG/DAO security issue was addressed in [34]. Here, the rate at which the tickle timer resets was limited through a specialized mechanism. However, certain critical issues persist for this work such as: no fixed threshold values, and node and network characteristics are not considered. Adaptive threshold based security mechanism was presented in [35] against DAG/DAO attacks. This mechanism improves upon the work presented in [34] in-terms of considering network characteristics. However, it still does not consider node characteristics. Another security mechanism was presented in [36] against DAG/DAO attack through dynamic approach. This mechanism further improves [35] by considering node characteristics.

The rank attack is caused when the malicious node advertises fake rank, in-order to attract significant traffic towards it. The main goal of rank attack is to establish non-optimal paths for routing. The security mechanism presented in [37] addresses the rank attacks. Here, hash operations are utilized to implement authentication. However, this mechanism still can become ineffective due to replay and forgery. Another security mechanism was presented in [38] to protect against rank attacks. The specialty of this mechanism is that, no cryptographic approach is utilized. However, there is still network size dependency.

The black hole attack is caused when the malicious node does not forward data packets which are routed towards it. Thus, essentially creating a object similar to black hole described in Astro-physics. Such attacks can result in significant increase in data loss due to reduced traffic. The security mechanism presented in [39] addresses black hole attack. However, this mechanism incurs significant overheads. Another security mechanism was presented in [40] against black hole attacks. The strength of this mechanism is that, even under attack, the throughput is maintained. However, there are still issues in identifying low rate attacks.

The sink-hole attack can further lead to different kinds of attacks such as: black holes, selecting forwarding, data tampering etc. Hence, the importance of sink-hole attack detection was outlined in [41]. Also, sink-hole detection mechanism based on link quality was presented in [41]. Even though this mechanism provides limited false positive rates, it suffers from significant overheads. This mechanism best suited for large networks. Another sink-hole detection mechanism was presented in [42]. This mechanism provides multiple merits such as: integrity, authentication and freshness. However, the effectiveness of this mechanism is still unsatisfactory.

The security mechanism presented in [43] -- indicated as Kinesis, specifically addresses data tampering attacks -- including selective forwarding and sink-hole attack. The merit of Kinesis is that, both attack identification and rectification is performed. However, this mechanism suffers due to redundant actions and hidden node issue.

From the presented literature survey, it is clear that, most of the security mechanisms presented against data tampering attack suffer from significant overhead issues, and there is significant scope to improve energy efficiency of robust encryption techniques such as 3DES, when they are applied to prevent data tampering attacks in WSN, and to address this outlined scope, the NNC scheme is presented in the next section.

III. OVERVIEW ON 3DES TECHNIQUE [17]

The 3DES technique is an extension of the DES technique which was designed in IBM during 1970s. The main features of DES encryption technique are: (1) The encryption key consists of 56 bits and these bits are selected through permutation scheme from initial 64 bits, and the left over 8 bits are converted into parity check bits or discarded. (2) The selected 56 bits are divided into two groups consisting of 28 bits each, and each group is subjected to separate

computation. (3) Through iterative computation, both groups are subjected to bit-left rotation operation, and 24 bits are selected from each group. (4) Finally, the selected and unselected bits from step 3 are merged to create final 56 bits for performing data encryption.

Even though, DES became popular and was widely utilized, it became easy to break the encryption scheme through brute force attack. Hence, to improve the security robustness of DES technique, the 3DES technique was presented in the literature. The 3DES technique utilizes three cryptographic keys of length 64 bits each. These cryptographic keys are denoted as secret keys, and are involved in both encryption and decryption of data. The formal details of these secret keys are described below.

Let, E_1, E_2 and E_3 indicate the encryption keys corresponding to first, second and third secret keys; similarly, D_1, D_2 and D_3 indicate the decryption keys corresponding to first, second and third secret keys; m indicate the data block which is subjected to encryption, and c indicate the encrypted form of m.

The encryption process of 3DES technique is represented in Equation 1 -- here, m is initially encrypted using E_1, and then, it is decrypted using D_2, and finally, it is encrypted using E_3 to produce c.

$$c = E_3(D_2(E_1(m))) \quad (1)$$

The decryption process of 3DES technique is represented in Equation 2 -- here, c is initially decrypted using D_3, and then, it is encrypted using E_2, and finally it is decrypted using D_1 to produce m.

$$m = D_1(E_2(D_3(c))) \quad (2)$$

Since, 168 bits are involved in the encryption and decryption process of 3DES technique, substantial computational effort is involved in achieving the encryption of data packets. Hence, directly applying 3DES encryption technique for encrypting WSN data packets can result in rapid energy loss -- especially, when large number of data packets need to be encrypted. The contemporary technique [17] directly applies 3DES encryption technique to encrypt WSN data packets, and this contemporary technique has to be optimized to achieve better energy efficiency, and this goal will be achieved through the proposed NNC scheme which is outlined in the next section.

IV. NNC SCHEME

4.1 Problem Formulation

Let, S indicate the source node, $S_N = [s_1, s_2, \ldots\ldots s_n]$ indicate the set of neighbor nodes for S, and D indicate the destination node or the base station. Here, S transmits its collected data packets to D, and D will forward these data packets to the IP network through available IP Gateways.

Let, $DP_S = [d_1, d_2, \ldots\ldots d_k]$ indicate the set of data packets of S which needs to be encrypted using 3DES encryption technique, and has to be transmitted to D. For each s_i ($1 \leq i \leq n$): re_i indicates the remnant energy of s_i -- here, re_i is normalized between [0,100] in which *0* and *100* indicate the lowest and highest remnant energy respectively; sa_i denotes the indicator random variable where only two values can be taken by it -- 1 and 100, 1 and 100 denote that, s_i is currently involved and not-involved in sensing activity respectively; ro_i denotes the indicator random variable where only two values can be taken by it -- 1 and 100, 1 and 100 denote that, s_i is currently involved and not-involved in routing activity respectively.

Let, $size(d_j)$ ($1 \leq j \leq k$) denote the data size in bytes of d_j, and $\text{expense}(s_i)$ denotes the energy expenditure of s_i in performing 3DES encryption on a single data byte -- here, $\text{expense}(s_i)$ is normalized between [0,100].

Let, $CS_r = (\hat{s}_1, \hat{s}_2, \ldots\ldots \hat{s}_k)$ denote a candidate solution for NNC scheme wherein; d_j is encrypted by $\hat{s}_j$. The merit of assigning d_j to $\hat{s}_j$ is evaluated through *NodeScore()*, which is represented in Equation 3 -- here, c_1, c_2 and c_3 indicate the tunable constants. Also, there is no restriction that, the nodes $\in CS_r$ should be distinct.

$$NodeScore(d_j, \hat{s}_j) = c_1\widehat{re}_j + c_2\widehat{sa}_j + c_3\widehat{ro}_j \quad (3)$$

When, d_j is encrypted by $\hat{s}_j$, corresponding update on $\widehat{re}_j$ is performed through *NodeUpdate()* as represented in Equation 4.

$$NodeUpdate(d_j, \hat{s}_j) = \widehat{re}_j - size(d_j)\text{expense}(\hat{s}_j) \quad (4)$$

The merit of each candidate solution such as CS_r is evaluated through *ScoreCS()* which is represented in Equation 5 -- here, $NodeScore(d_j, \hat{s}_j | CS_r - \hat{s}_j)$ calculates $NodeScore(d_j, \hat{s}_j)$ by considering the nodes $\in (CS_r - \hat{s}_j)$ have already performed their encryption and corresponding *NodeUpdate()* operations have been executed by all the nodes $\in (CS_r - \hat{s}_j)$. It must be noted that, higher values of *ScoreCS()* indicates that, the corresponding candidate solutions provide more beneficial solutions to the NNC scheme.

$$ScoreCS(CS_r) = \sum_{j=1}^{k} NodeScore(d_j, \hat{s}_j | CS_r - \hat{s}_j) \quad (5)$$

Theorem 1. *The candidate solution which maximizes Equation 5 provides the optimal solution for the NNC scheme*.

Proof. Suppose, CS_o is the candidate solution obtained by maximizing Equation 5, and CS_r is the optimal candidate solution. Assuming, $CS_o \neq CS_r$ and $CS_o < CS_r$ -- however, from the Equation 5 it is clear that, *ScoreCS()* belongs to the class of monotonic functions, and this assumption cannot be valid which immediately proves the Theorem.

Theorem 2. *The searching problem to find the optimal candidate solution which maximizes Equation 5 has non-polynomial complexity*.

Proof. The number of distinct nodes involved in the candidate solution varies from *1* to *k*, because there is no restriction of nodes $\in CS_r$ should be distinct. So, the number of candidate solutions which can be possibly created is bounded by $\geq k + \binom{k}{2} + \binom{k}{3} + \cdots \binom{k}{k}$, which immediately proves the Theorem.

Theorem 1 outlines that, the optimal solution to the NNC scheme is obtained through the maximization of Equation 5 WRT CS_r. However, Theorem 2 states that, the searching problem to find the candidate solution which maximizes Equation 5 has non-polynomial complexity; hence, approximate solution techniques which run in polynomial complexity and provide approximate solutions which are closer to the optimal solution need to be designed, and this technique is presented below.

4.2 Algorithm

Algorithm 1 *RTNNC (S, D, S_N, DP_S)*

For $(j = 1; j \leq k; j++)$

$flag_j = 0$

EndFor

EncryptedList=CreateEmptyList()

For $(j = 1; j \leq k; j++)$

For $(i = 1; i \leq n; i++)$

If $(rand(0,1) \leq P_{ji})$

TransmitPacket(S, s_i, d_j)

EncryptPacket3DES(s_i, d_j)

TransmitPacket(s_i, S, d_j)

Add(EncryptedList, d_j)

$flag_j = 1$

Break

EndIf

EndFor

EndFor

For $(j = 1; j \leq n; j++)$

If $(flag_j == 0)$

EncryptPacket3DES(S, d_j)

Add(EncryptedList, d_j)

$flag_j = 1$

EndIf

EndFor

Return *EncryptedList*

The approximate solution technique for the NNC scheme is designed through randomized algorithm which is outlined in Algorithm 1, which is indicated as Randomized Technique for NNC (RTNNC). The description of RTNNC is outlined below.

Initially, all the data packets $\in DP_S$ are marked through $flag_j$ in-order to indicate that, the encryption of these data packets is pending. An empty list indicated as *EncryptedList* is created through *CreateEmptyList()* in-order to store the encrypted data packets. Each data packet or $d_j \in DP_S$ is considered sequentially for encryption, and to encrypt this data packet each $s_i \in S_N$ is considered sequentially. The probability of encrypting d_j by s_i is calculated through $P(d_j, s_i)$ or P_{ji} which is represented in Equation 6.

$$P(d_j, s_i) = P_{ji} = \frac{c_1 re_i + c_2 sa_i + c_3 ro_i}{100(c_1 + c_2 + c_3)} \quad (6)$$

If the value of the random number generator function indicated by *rand*() which generates numbers between 0 and 1, is $\leq P_{ji}$ then this event indicates that encryption of d_j should be performed through s_i. Hence to accomplish this encryption: (1) d_j is transmitted to s_i by S through *TransmitPacket();* (2) s_i performs 3DES encryption of d_j through *EncryptPacket3DES()* and this function also executes *NodeUpdate()* for updating about s_i for encrypting d_j*;* (3) d_j which is in encrypted format is transmitted back to S by s_i through *TransmitPacket();* (4) d_j is added to the *EncryptedList* using *Add();* (5) finally, $flag_j$ is set to 1.

After considering every $d_j \in DP_S$ for performing encryption through the aid of nodes $\in S_N$, if some of the data packets still have not been encrypted which is identified through $flag_j$, such data packets are eventually encrypted by S through *EncryptPacket3DES()* and added to *EncryptedList* using *Add().* Finally, *EncryptedList* is returned by Algorithm 1.

Let CS_o indicate the optimal candidate solution of the NNC scheme. The Theorem 3 outlines the fact that, Algorithm 1 discovers or utilizes CS_o for encryption of all the data packets $\in DP_S$ based on certain probability, and the details of the corresponding probability mass function are presented in next Theorem.

Theorem 3. *Algorithm 1 belongs to the class of Monte-Carlo randomized algorithms.*

Proof. Each node $\in CS_o$ is selected for encryption by Algorithm 1 based on probability which is represented in Equation 6. Hence, selection of all the nodes $\in CS_o$ by Algorithm 1 for encryption of all the data packets $\in DP_S$ is again based on probability which immediately proves the Theorem.

Let, the probability of choosing CS_r which is one of the candidate solutions of the NNC scheme by Algorithm 1 for encrypting all the data packets $\in DP_S$ be indicated by $P(CS_r)$. The Theorem 4 outlines the upper bound on the metric $P(CS_r)$.

Theorem 4. *The metric $P(CS_r)$ is upper bounded as represented in Equation 7.*

Proof. Algorithm 1 selects s_i for encrypting d_j through a Bernoulli trial wherein; the success probability of this Bernoulli trial is represented in Equation 6. Also, each Bernoulli trial is independent of the others. Hence, by using the law of joint probability of independent Bernoulli trials, the Theorem immediately follows.

$$P(CS_r) \leq \prod_{j=1}^{k} P(d_j, \hat{s}_j) \quad (7)$$

The Theorem 5 outlines the relationship between Equations 5 and 7.

Theorem 5. *If $CS_r \neq CS_z$ and $ScoreCS(CS_r) \leq ScoreCS(CS_z)$ then, $P(CS_r) \leq P(CS_z)$*

Proof. Since, the LHS of both Equations 5 and 7 take only non-negative values, and by comparing both these Equations, it is clear that, the Theorem immediately follows.

Theorem 6 asserts that, CS_o has the highest probability for being selected by Algorithm 1 for encryption of all the data packets $\in DP_S$.

Theorem 6. $P(CS_r) \leq P(CS_o)$ *where* $CS_r \neq CS_o$

Proof. Since, CS_o is the optimal candidate solution of the NNC scheme, implying that $ScoreCS(CS_r) \leq ScoreCS(CS_o)$. Hence, by using Theorem 5, this Theorem immediately follows.

Theorem 7 asserts the fact that, if the resource capabilities of each node $\in CS_o$ is high, then, Algorithm 1 has higher chances of selecting CS_o for encryption of all the data packets $\in DP_S$.

Theorem 7. *If the values $(\widehat{re}_j, \widehat{sa}_j, \widehat{so}_j)$ for each $\hat{s}_j \in CS_o$ are high, then, $P(CS_o)$ will have higher values.*

Proof. By analyzing Equation 6, it is clear that, if the values $(\widehat{re}_j, \widehat{sa}_j, \widehat{so}_j)$ are high, then, $P(d_j, \hat{s}_j)$ will have higher values, and correspondingly by analyzing Equation 7 it is clear that, $P(CS_o)$ will have higher value.

The Theorems 8 and 9 assert that, Algorithm 1 rarely selects candidate solutions which are having limited resources.

Theorem 8. *If for some CS_r where $CS_r \neq CS_o$ and $ScoreCS(CS_r)$ has low value, then, $P(CS_r)$ also has lower value.*

Proof. The proof for this Theorem is a direct consequence of Theorem 5. Hence, this Theorem immediately follows.

Theorem 9. *If for some CS_r where $CS_r \neq CS_o$ and the values $(\widehat{re}_j, \widehat{sa}_j, \widehat{so}_j)$ for each $\hat{s}_j \in CS_r$ are low, then, $P(CS_r)$ will have lower value.*

Proof. The proof for this Theorem is a direct consequence of Theorem 7. Hence, this Theorem immediately follows.

The Theorem 10 asserts that, the computational complexity of Algorithm 1 is polynomial.

Theorem 10. *Algorithm 1 has polynomial time complexity.*

Proof. Algorithm 1 considers each data packet $\in DP_S$ sequentially, and to encrypt each data packet, it considers the nodes $\in S_N$ also sequentially. Since, $|S_N| = n$ and $|DP_S| = k$, it implies that, the execution complexity of Algorithm 1 can be bounded by $O(\max(k, n)^2)$ which immediately proves the Theorem.

Theorems 6, 7, 8 and 9 establish the effectiveness of Algorithm 1 in utilizing candidate solution for the NNC scheme which has good resources. Theorem 10 establishes the efficiency of Algorithm 1 in-terms of polynomial complexity. Thus, Algorithm 1 achieves its dual objective of effectiveness and execution efficiency.

The system design flow diagram for implementing the NNC scheme is illustrated in Figure 1. There are five components involved in implementing the NNC scheme. The *Node Statistics Collector* component is responsible for collecting the node statistics required for NNC scheme which includes source node and all its corresponding neighbors. The *Executor* component is responsible for executing Algorithm 1 with the aid of *Encryption* component which performs the required 3DES encryption of data packets. The *Node Statistics Updater* component is responsible for collecting the current information of those nodes which have been involved in the NNC scheme, and update this information in *Node Statistics Collector* component. The *Executor* continuously procures information from the *Node Statistics Collector* component in-order to utilize the current node information for executing Algorithm 1. Finally, the *Executor* routes the encrypted data packets to the Base Station through the *Transmitter* component.

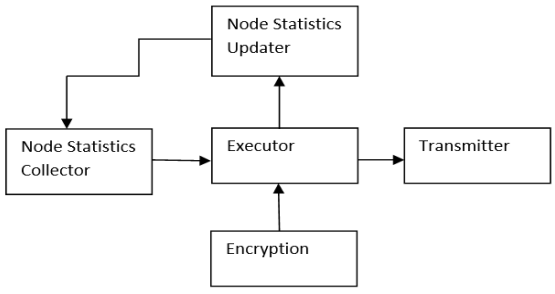

Figure 1: System Design Flow Diagram

V. RESULTS AND DISCUSSIONS

5.1 Simulation Setup

The proposed NNC scheme is simulated in MATLAB, and for the ease of reference, the proposed scheme will be denoted as *NNC*. The contemporary technique outlined in [17] is also simulated along with NNC, and for the ease of reference, this contemporary technique will be denoted as *COT*. The simulation settings are outlined in Table 1.

Table 1: Simulation Parameter Settings

Simulation Parameters	Used Values
$\|S_N\|$	Varied between [10,100]
$\|DP_S\|$	Varied between [10,100]
re_i	Varied between [1,100]
sa_i	Either 1 or 100
ro_i	Either 1 or 100
$size(d_j)$	Varied between $[10^3, 10^4]$
$expense(s_i)$	Varied between $[10^{-3}, 10^{-4}]$
c_1	2
c_2	1
c_3	1

The performance metric used in the simulation study analysis is denoted as *Average Energy Consumption* (*AVEC*), and it is represented in Equation 8: here, $TSize(s_i)$ is the total size of all the data packets encrypted by $s_i \in S_N$; s_i should be involved in the encryption of at-least one data packet; $\bar{S}_N$ contains those nodes of S_N which have involved in the encryption of at-least one data packet; $I(\bar{S}_N)$ denotes the indicator variable which takes either of the two values $|\bar{S}_N| + 1$ or $|\bar{S}_N|$ depending whether S is involved in the encryption of at-least one data packet or otherwise respectively. Clearly for COT, $|S_N| = 0$, because all the data packets are encrypted by S. The metric AVEC highlights the average energy consumed by each node $\in S_N$ in encrypting the data packets $\in DP_S$. Clearly, higher values of AVEC indicate that, the utilized technique is node-energy inefficient, and can result in rapid node energy drainage.

$$AVEC = \frac{\sum_i expense(s_i)TSize(s_i) + expense(S)TSize(S)}{I(\bar{S}_N)} \quad (8)$$

In-order to study the influence of AVEC on: re_i, sa_i and so_i, three metrics are defined respectively. The first metric is denoted as $R(re_i)$ which indicates the ratio of those nodes $\in S_N$ which have their corresponding value for $re_i = 100$. The second metric is denoted as $R(sa_i)$ which indicates the ratio of those nodes $\in S_N$ which have their corresponding value for $sa_i = 100$. The third metric is denoted as $R(so_i)$ which indicates the ratio of those nodes $\in S_N$ which have their corresponding value for $so_i = 100$. Clearly, higher values of $R(re_i)$, $R(sa_i)$ and $R(so_i)$ indicate that S_N contains resource rich nodes.

5.2 Discussions on Simulation Results

The first simulated experiment analyzes the performance of COT and NNC WRT AVEC when $|S_N|$ is varied and other simulation parameters are kept constant. The result analysis of the first simulated experiment is illustrated in Figure 2, and the following observations are made: (1) since, S_N has no influence on COT, the performance of COT remains constant. (2) NNC substantially outperforms COT primarily due to its encryption load sharing design. (3) The performance of NNC is positively correlated with $|S_N|$, because as the number of neighbor nodes of *S* increase, the encryption load distribution becomes more effective.

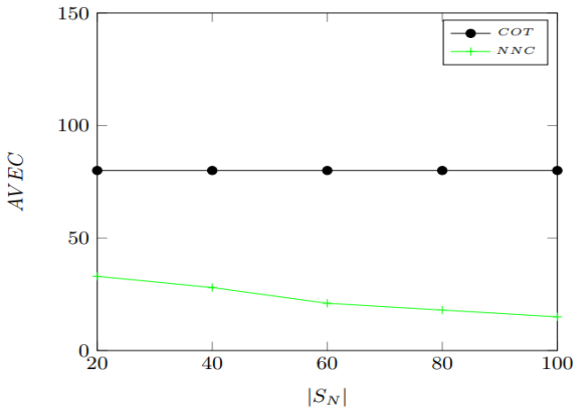

Figure 2: $|S_N|$ vs *AVEC*

The second simulated experiment analyzes the performance of COT and NNC WRT AVEC when $|DP_S|$ is varied and other simulation parameters are kept constant. The result analysis of the second simulated experiment is illustrated in Figure 3, and the following observations are made: (1) the performance of COT suffers mainly due to lack of encryption load sharing mechanism. (2) The performance of COT is negatively correlated with $|DP_S|$ because as the number of data packets increase, resource investment for data packet encryption also increases. (3) NNC provides substantial performance improvement over COT for the same reason outlined in Observation (2) for the first simulated experiment. (4) The performance of NNC is negatively correlated with $|DP_S|$ because of the same reason outlined in Observation (2).

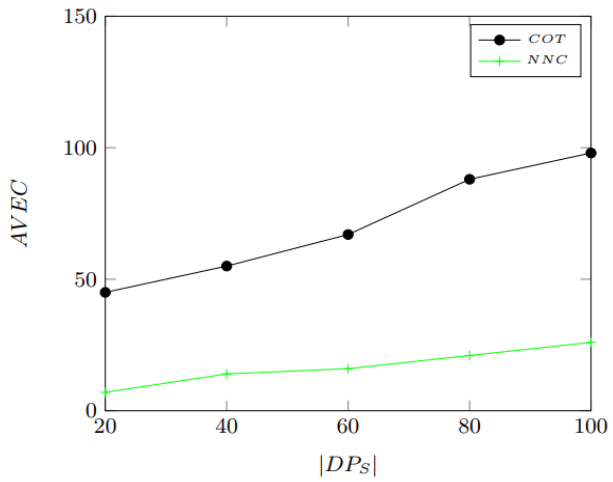

Figure 3: $|DP_S|$ vs *AVEC*

In-order to perform the third simulated experiment, $size(d_j)$ for all the data packets $\in DP_S$ is kept constant. Specifically, the third simulated experiment analyzes the performance of NNC and COT WRT AVEC when $size(d_j)$ is varied and other simulation parameters are kept constant. The result analysis of the third simulated experiment is illustrated in Figure 4, and the following observations are made: (1) the performance of COT suffers for the same reason outlined in Observation (1) for second simulated experiment. (2) The performance of COT is negatively correlated with $size(d_j)$, because as the size of data packets increase, corresponding increase in resource investment is required for encryption. (3) The performance of NNC is substantially superior compared to COT for the same reason outlined in Observation (2) of the first simulated experiment. (4) The performance of NNC is negatively correlated with $size(d_j)$ for the same reason outlined in Observation (2).

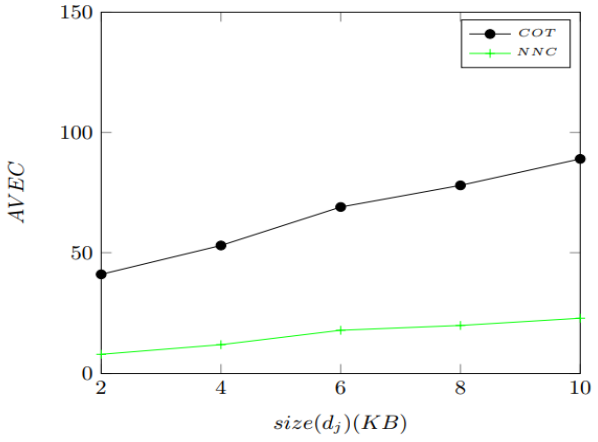

Figure 4: $size(d_j)$ vs *AVEC*

The fourth simulated experiment analyzes the performance of NNC and COT WRT AVEC when $R(re_i)$ is varied and all other simulation parameters are kept constant. The result analysis of the fourth simulated experiment is illustrated in Figure 5, and the following observations are made: (1) the performance of COT remains constant because $R(re_i)$ has no influence on COT. (2) NNC substantially outperforms COT for the same reason outlined in Observation (2) of the first simulated experiment. (3) The performance of NNC is positively correlated with $R(re_i)$, because as the number of neighbor nodes $\in S$ having complete remnant energy increases, the encryption load distribution also becomes more effective due to rich resource availability in the neighbor nodes of *S*.

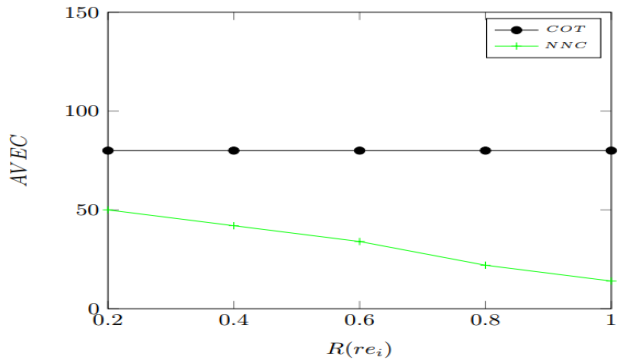

Figure 5: $R(re_i)$ vs *AVEC*

The fifth simulated experiment analyses the performance of NNC and COT WRT AVEC when $R(sa_i)$ is varied and all other simulation parameters are kept constant. The result analysis of the fifth simulated experiment is illustrated in Figure 6, and the following observations are made: (1) The performance of COT remains constant because $R(sa_i)$ has no influence on COT. (2) NNC exhibits substantially performance mileage over COT for the same reason outlined in Observation (2) of the first simulated experiment. (3) The performance of NNC is positively correlated with $R(sa_i)$, because as the number of nodes having $sa_i = 100$ increases, the encryption load distribution effectiveness increases due to rich resource availability in the neighbor nodes of *S*.

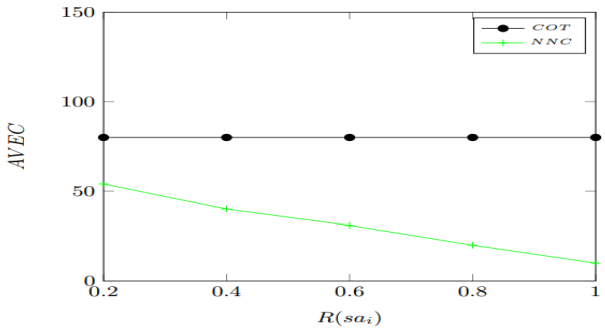

Figure 6: $R(sa_i)$ vs *AVEC*

The sixth simulated experiment analyzes the performance of NNC and COT WRT AVEC when $R(ro_i)$ is varied and all other simulation parameters are kept constant. The result analysis of the sixth simulated experiment is illustrated in Figure 7, and the following observations are made: (1) The performance of COT remains constant because $R(ro_i)$ has no influence on COT. (2) The relatively superior performance of NNC over COT is due to the same reason outlined in Observation (2) of the first simulated experiment. (3) The performance of NNC is positively correlated with $R(ro_i)$, because as the number of nodes having $ro_i = 100$ increases, the encryption load distribution effectiveness increases due to rich resource availability in the neighbor nodes of S.

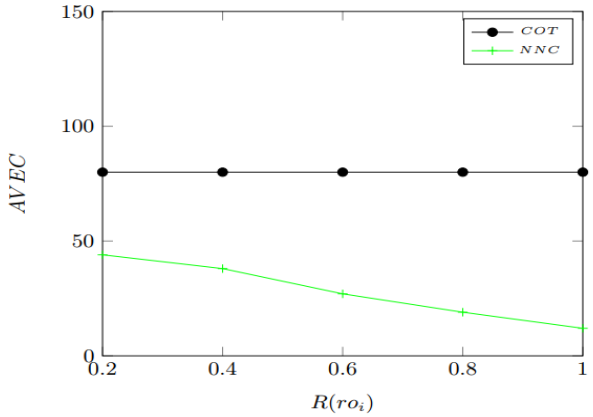

Figure 7: $R(ro_i)$ vs *AVEC*

VI. CONCLUSION AND FUTURE SCOPE

In this paper, the main open issue of performing WSN data packet encryption by incurring limited energy expenditure was addressed through the NNC scheme. The NNC scheme was modeled as an optimization problem, which was shown as having non-polynomial complexity. A randomized algorithm was presented to approximately solve the optimization problem. The proposed encryption scheme was simulated and compared against the contemporary technique. In the outlined simulation analysis study, the proposed encryption scheme relatively and substantially outperformed the contemporary technique in-terms of data packet energy expenditure.

The main limitation of the proposed NNC scheme is that, the routing nodes are not utilized for sharing the encryption load. It must be noted that, the Quality of Service (QoS) based routing nodes, usually have significant computational resources, and which can be utilized to share the encryption load of the source node. Including the QoS based routing nodes in the NNC scheme can further improve the encryption load distribution efficiency, and due to which, the energy expenditure for data packet encryption can be further reduced. However, the main challenge is to reformulate the formal models used in the NNC scheme to include these QoS based routing nodes.

REFERENCES

[1] J. A. Stankovic, *"Research directions for the Internet of Things," IEEE Internet Things J.*, vol. 1, no. 1, pp. 3–9, Feb. 2014.

[2] P. Rawat, K. D. Singh, H. Chaouchi, and J. M. Bonnin, "*Wireless sensor networks: A survey on recent developments and potential synergies," J. Supercomput.*, vol. 68, no. 1, pp. 1–48, 2014.

[3] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, *"Cyber-physical systems: The next computing revolution,"* in *Proc. 47th Design Autom. Conf.*, Anaheim, CA, USA, 2010, pp. 731–736.

[4] F. Mattern and C. Floerkemeier, *"From the Internet of computers to the Internet of Things,"* in *From Active Data Management to Event-Based Systems and More*. Berlin, Germany: Springer, 2010, pp. 242–259.

[5] Y. Mo *et al.*, *"Cyber-physical security of a smart grid infrastructure," Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[6] S. Ali *et al.*, *"Network challenges for cyber physical systems with tiny wireless devices: A case study on reliable pipeline condition monitoring," Sensors*, vol. 15, no. 4, pp. 7172–7205, 2015.

[7] M. M. Hossain, M. Fotouhi, and R. Hasan, *"Towards an analysis of security issues, challenges, and open problems in the Internet of Things,"* in *Proc. IEEE World Congr. Services*, New York, NY, USA, 2015, pp. 21–28.

[8] S. Sicari, A. Rizzardia, L. A. Griecob, and A. Coen-Porisini, *"Security, privacy and trust in Internet of Things: The road ahead," Comput. Netw.*,vol. 76, pp. 146–164, Jan. 2015.

[9] Y. Wang, G. Attebury, and B. Ramamurthy, *"A survey of security issues in wireless sensor networks," IEEE Commun. Surveys Tuts.*, vol. 8, no. 2, pp. 2–23, 2nd Quart., 2006.

[10] C. M. Medaglia and A. Serbanati, *"An overview of privacy and security issues in the Internet of Things,"* in *The Internet of Things*. New York, NY, USA: Springer, 2010.

[11] J. S. Kumar and D. R. Patel, *"A survey on Internet of Things: Security and privacy issues," Int. J. Comput. Appl.*, vol. 90, no. 11, pp. 20–26, 2014.

[12] J. Lin *et al.*, *"A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2017.2683200.

[13] J. Granjal, E. Monteiro, and J. S. Silva, *"Security for the Internet of Things: A survey of existing protocols and open research issues," IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.

[14] A. Bröring *et al.*, *"New generation sensor Web enablement," Sensors*, vol. 11, no. 3, pp. 2652–2699, 2011.

[15] K. Sohrabi, J. Gao, V. Ailawadhi, and G. J. Pottie, *"Protocols for self organization of a wireless sensor network," IEEE Pers. Commun.*, vol. 7, no. 5, pp. 16–27, Oct. 2000.

[16] *"International electrotechnical commission, Internet of Things: Wireless sensor networks,"* White Paper, 2014.

[17] G. S. Prathamesh, G. D. Sanket, K. D. Yogeshwar, and N. K. Aniket, *"Secure Data Transmission in WSN using 3DES with Honey Encryption*", IJARIIE, vol. 1, pp. 455-461, 2015.

[18] C. P. O'Flynn, *"Message denial and alteration on IEEE 802.15.4 low power radio networks,"* in *Proc. 4th IFIP Int. Conf. New Technol.Mobility Security*, Paris, France, 2011, pp. 1–5.

[19] Y. Xiao, S. Sethi, H.-H. Chen, and B. Sun, *"Security services and enhancements in the IEEE 802.15.4 wireless sensor networks,"* in

Proc. IEEE Glob. Telecommun. Conf., St. Louis, MO, USA, 2005, pp. 1976–1980.

[20] Y. W. Law *et al.*, *"Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols," ACM Trans. Sensor Netw.*,vol. 5, no. 1, 2009, Art. no. 6.

[21] D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, *"Effects of denial-of-sleep attacks on wireless sensor network MAC protocols," IEEE Trans. Veh. Technol.*, vol. 58, no. 1, pp. 367–380, Jan. 2009.

[22] H. Kim, *"Protection against packet fragmentation attacks at 6LoWPAN adaptation layer,"* in *Proc. Int. Conf. Converg. Hybrid Inf. Technol.*, Daejeon, South Korea, 2008, pp. 796–801.

[23] R. Hummen *et al.*, *"6LoWPAN fragmentation attacks and mitigation mechanisms,"* in *Proc. 6th ACM Conf. Security Privacy Wireless Mobile Netw.*, Budapest, Hungary, 2013, pp. 55–66.

[24] L. M. L. Oliveira, J. J. P. C. Rodrigues, A. F. de Sousa, and J. Lloret, *"A network access control framework for 6LoWPAN networks," Sensors*, vol. 13, no. 1, pp. 1210–1230, 2013.

[25] E. J. Cho, J. H. Kim, and C. S. Hong, *"Attack model and detection scheme for botnet on 6LoWPAN,"* in *Proc. 12th Asia–Pac. Netw. Oper.Manag. Conf.*, Jeju-do, South Korea, 2009, pp. 515–518.

[26] L. Wallgren, S. Raza, and T. Voigt, *"Routing attacks and countermeasures in the RPL-based Internet of Things," Int. J. Distrib. Sensor Netw.*, vol. 9, no. 8, pp. 1–11, 2013.

[27] K. Heurtefeux, O. Erdene-Ochir, N. Mohsin, and H. Menouar, *"Enhancing RPL resilience against routing layer insider attacks,"* in *Proc. IEEE 29th Int. Conf. Adv. Inf. Netw. Appl.*, Gwangju, South Korea, 2015, pp. 802–807.

[28] S. Raza, L. Wallgren, and T. Voigt, *"SVELTE: Real-time intrusion detection in the Internet of Things," Ad Hoc Netw.*, vol. 11, no. 8, pp. 2661–2674, 2013.

[29] F. I. Khan, T. Shon, T. Lee, and K. Kim, *"Wormhole attack prevention mechanism for RPL based LLN network,"* in *Proc. 5th Int. Conf.Ubiquitous Future Netw.*, 2013, pp. 149–154.

[30] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, and L. W. Chang, *"Preventing wormhole attacks on wireless ad hoc networks: A graph theoretic approach,"* in *Proc. IEEE Wireless Commun. Netw. Conf.*, vol. 2. New Orleans, LA, USA, 2005, pp. 1193–1199.

[31] E. C. H. Ngai, J. Liu, and M. R. Lyu, *"On the intruder detection for sinkhole attack in wireless sensor networks,"* in *Proc. IEEE Int. Conf.Commun.*, Istanbul, Turkey, 2006, pp. 3383–3389.

[32] K. Weekly and K. Pister, *"Evaluating sinkhole defense techniques in RPL networks,"* in *Proc. 20th IEEE Int. Conf. Netw. Protocols*, Austin, TX, USA, 2012, pp. 1–6.

[33] J. Newsome, E. Shi, D. Song, and A. Perrig, *"The Sybil attack in sensor networks: Analysis & defenses,"* in *Proc. 3rd Int. Symp. Inf. Process.Sensor Netw.*, Berkeley, CA, USA, 2004, pp. 259–268.

[34] J. Hui and J. P. Vasseur, *"The routing protocol for low-power and lossy networks (RPL) option for carrying RPL information in data-plane datagrams,"* Internet Eng. Task Force, Fremont, CA, USA, RFC 6553, 2012. [Online]. Available: https://tools.ietf.org/html/rfc6553

[35] A. Sehgal, A. Mayzaud, R. Badonnel, I. Chrisment, and J. Schönwälder, *"Addressing DODAG inconsistency attacks in RPL networks,"* in *Proc.Glob. Inf. Infrastruct. Netw. Symp.*, Montreal, QC, Canada, 2014, pp. 1–8.

[36] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schönwälder, *"Mitigation of topological inconsistency attacks in RPL-based lowpower lossy networks," Int. J. Netw. Manag.*, vol. 25, no. 5, pp. 320–339, 2015.

[37] A. Dvir, T. Holczer, and L. Buttyan, *"VeRA—Version number and rank authentication in RPL,"* in *Proc. IEEE 8th Int. Conf. Mobile Ad Hoc Sensor Syst.*, Valencia, Spain, 2011, pp. 709–714.

[38] M. Landsmann, M. Wahlisch, and T. C. Schmidt, *"Topology authentication in RPL,"* in *Proc. IEEE Conf. Comput. Commun. Workshops*, Turin, Italy, 2013, pp. 73–74.

[39] R. Venkataraman, S. Moeller, B. Krishnamachari, and T. R. Rao, *"Trustbased backpressure routing in wireless sensor networks," Int. J. Sensor Netw.*, vol. 17, no. 1, pp. 27–39, 2015.

[40] Z. Lu, Y. E. Sagduyu, and J. H. Li, *"Securing the backpressure algorithm for wireless networks," IEEE Trans. Mobile Comput.*, vol. 16, no. 4, pp. 1136–1148, Apr. 2017.

[41] F.-J. Shang, C. Li, and J.-L. Qin, *"Improvement of approach to detect sinkhole attacks in wireless sensor networks,"* in *Computer, Intelligent Computing and Education Technology*. Boca Raton, FL, USA: CRC Press, 2014, pp. 695–698.

[42] P. Pecho, P. Hanacek, and J. Nagy, *"Simulation and evaluation of CTP and secure-CTP protocols," Radioengineering*, vol. 19, no. 1, pp. 89–99, 2010.

[43] S. Sultana, D. Midi, and E. Bertino, *"Kinesis: A security incident response and prevention system for wireless sensor networks,"* in *Proc. 12th ACM Conf. Embedded Netw. Sensor Syst.*, Memphis, TN, USA, 2014, pp. 148–162.

Author's Profile

Mrs.V.Gayathri pursued Bachelor of Science from Gulbarga University, Bellary in 2002 and Master of Science from Gulbarga University in year 2004. She is currently pursuing Ph.D in Rayalaseema University. She is currently working as Assistant Professor in Department of Computer Science, Govt.Science College Bengaluru, India since 2014. She is a member of CSI since 2013. She has published more than 6 research papers in reputed international journals and conferences including IEEE. Her main research work focuses on Cryptography, Network Security, Wireless Sensor Network and Privacy, Data Mining, IoT. She has 13 years of teaching experience and 4 years of Research Experience.

Dr Y S Kumaraswamy currently working as Professor & Dean R&D in Department of Computer Science & Engineering, NCET Bengaluru, India Since 2016. He is a member of IEEE & IEEE computer society since 2013, He has published more than 150 research papers in reputed international journals including Thomson Reuters (SCI & Web of Science) and conferences including IEEE and it's also available online. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Computational Intelligence based education. He has 30 years of teaching experience and 20 years of Research Experience. guided Many Ph.D students in the area of Computer Science and also selection committee member for ISRO/UGC/DST.

