International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-5, March 2020

Novel Framework for Maximizing Security over Wireless Network

Tejashwini N, D R Shashi Kumar, K Satyanarayana Reddy

Abstract*: With the increasing adoption of application running over wireless networking system, there is also an increasing security concern in it. Review of existing security protocols in wireless networks shows that they are highly specific to adversaries and hence they cannot be applicable with the dynamic state of network vulnerabilities. Apart from this, it was also explored that public key encryption requires a drastic change in its design methodology in order to make it more resource friendly for increased network lifetime. Therefore, this manuscript presents a novel framework that develops an enhanced model of public key encryption using algebraic structure that can generate an elite secret key. The study also introduces a design of an efficient trapdoor function which renders maximum resiliency towards different forms of lethal attacks as well as adhere to maximum security standards in wireless network. The study outcome shows that proposed system out performs frequently used existing security standards in many aspects.

Keywords: Attacks, Public Key Cryptography, Security, Wireless network

I. INTRODUCTION

Adoption of wireless network is now very much common in almost everywhere right from domestic to commercial usage [1]. Although, it offers much flexibility in accessing data using mobile nodes; however, it also invites various vulnerable situations. One of the biggest concerns in wireless network is to carry out forwarding of the data from transmitting device to the target destination node. In order to offer security, there are availability of various encryption mechanisms in order to secure the communication in wireless network [2]-[5]. Usually, the cryptography process assists in performing encryption of the plain text message from the original message with the assistance of secret key. The encrypted data can be securely transmitted to the destination node in this process. The next process is related to the decryption that is carried out by the destination node which results in discloser of the original data. In all this process the secret key is basically used for securing the encryption technique and thereby protects transmitting and receiving nodes However, this is not that easy as it seems like. At present, there are various security protocols being evolved in wireless network but all the protocols are not claimed to offer full fledge security [6]. There are various reason behind it viz. i) the wireless nodes are basically characterized by low resources and lower processing capabilities and hence they are not in a position to support the complex encryption protocol and ii) security protocols in wireless network are again of various types and forms which is developed on the basis of resistivity to specific form of attack or specific environment, iii) adoption of any cryptographic protocol will have a dependency to store the secret keys, which are usually stored within the nodes. This saturates the buffer of the node soon and the node suffers from communication degradation problems. In short, existing cryptographic measures are not sufficient to offer a good balance between communication performance upgradation and computational efficiency. Another biggest problem associated with existing security protocols is that they are actually not resource friendly. In order to offer better security performance, there is always a higher demand of energy and node sustainability. If the network works on smaller scale, such problems doesn't matter; however, if the problem is in larger scale than it affects both communication and security. It gives rise to interference as well as overhearing, which also open up the scope of adversary to initiate an attack. Therefore, there is always a need of security algorithm which has lesser consumption of resources. There are few ways which can ensure that viz. i) generation technique of secret key should be improved, ii) the network should be able to process in larger scale of noes, and iii) maximize connectivity and coverage. All these demand higher ranges of energy while performing security operation. All this are quite essential to be considered as if the adversary is strong than an effective algorithm should be design. At present, there are various ranges of attackers that intrude wireless network and the score is exponentially increasing [7][8]. It has been observed that public key encryption is widely adopted in existing security approaches on wireless network [9]. Although, public key approaches has significant benefits in wireless network, but it is also shrouded with various flaws. One of the significant problems in public key encryption methods is that it generates larger sizes of secret key. It is highly detrimental for large scale and distributed wireless network. Therefore, this manuscript presents a novel solution that is meant for maximizing the security features in wireless network with higher resistance towards majority of threats in it. Section II discusses about the existing followed by research problem in Section III. Research Methodology is discussed in Section IV followed by Algorithm implementation in Section V.

Revised Manuscript Received on March 30, 2020.
* Correspondence Author
Tejashwini N*, Research Scholar, Visvesvaraya Technological University, Belagavi, Karnataka, India. Email: tejashwini.n@gmail.com
Dr. D R Shashi Kumar**, Head of Department of Computer Science & Engineering, Cambridge Institute of Technology, Bengaluru, Karnataka, India
Dr. K Satyanarayana Reddy***, Head of Department of Information Science & Engineering, Cambridge Institute of Technology, Bengaluru, Karnataka, India

Result analysis is discussed in Section VI while the summary of paper in briefed in Section VII as conclusion.

II. RELATED WORK

This section updates about the security schemes as a following of our prior work [10]. Most recently, the work carried out by Nguyen et al. [11] has presented a discussion about the security breach owing to the depletion of energy. The author has addressed the problem associated with *security concern of the wireless network* especially which is equipped with low-powered nodes. This is basically a review-based work to claim that energy-based attacks are most vulnerable form of attacks. From the wireless network perspective, Internet-of-Things (IoT) is also getting popular to assists in establishing massive connection with various devices using wireless networking protocols. Such networks are more vulnerable for variable unknown attacks. Studies in this direction have been carried out by Ding et al. [12] where the problems associated with *errors due to channel estimation* and *eavesdropping* is emphasized. The solution offered by authors is based on applying probability-based solution where a reliable computation is carried out for channel estimates. The study is more focused on physical layer security. Another study where energy is associated with the security in wireless network is carried out by Iliad and Al-Ahmadi [13]. The study has focused on the problem associated with *wormhole attack* where the solution is presented on the basis of using an on-demand routing scheme developed over network simulator. The study outcome exhibited higher accuracy of detection and also claimed of cost effectiveness. The work carried out by Han et al. [14] has addressed the problem of security due to *network with higher instability* and restricted resources. The author has presented an assessment of the quantitative parameter using swarm intelligence integrated with convolution neural network. The mechanism assists in identifying the exact feature in order to perform detection of malicious node. The work carried out by Tsiota et al. [15] has mitigated the problem associated with *black hole attack* and *jamming attack* considering the case study of heterogeneous network. The study has used Poisson process over multiple tier with information about regular and malicious nodes using probability concept. Vashist et al. [16] have developed an analytical model for resisting *denial-of-service attack* along with *jamming attack*. The solutions for this is presented using correction code with burst error as well as the authors have also deployed a unique classification approach using machine learning. The study outcome showcase that there was good utilization of resource with optimistic attack identification.

From the security viewpoint, another frequently considered factor is trust. The work carried out by Yun et al. [17] have emphasized on the attacks related to the *packet drop* in wireless network. According to the work, a reliable centralized system has been developed in order to carry out secure transmission of data packet over wireless network on the basis of the computed trust factor. Fang et al. [18] have developed an algorithm that reviews the existing approaches connected to the state of security schemes in 5G technologies. Finally, the authors have also presented a solution using authentication-based approach along with identify factors of the nodes in 5G communication system. Guan and Ge [19] have addressed the problem related to the *injection of malicious data* over the cyber physical system along with *jamming* attack. The idea is to capture the event of attack considering the case study of sensor network using mathematical probability measures. The solution has also implemented detection of attack using estimation of the significant factors towards distributed attacks. Guan and Ge [20] have implemented a scenario where there are multiple attacks mainly of *jamming types*. The authors have presented a Markov chain of homogeneous nature in order to resist such form of attack. The study has also formulated a mechanism for estimating the vulnerability of the target signal considering the multichannel transmission.

Study towards resisting *jamming attack* was also carried out by Heo et al. [21] thereby offering solution to resist such stealthy form of attacks. The authors have presented an anti-jamming process which is more suitable for energy-restricted devices working over wireless network of lossy nature. The idea offers security to the conformity message on the basis of the actual data packet contents. It is also claimed capable of retrieved jammed packets. Ever [22] have presented an authentication scheme in order to maintain privacy of the user associated with the healthcare. The study addresses the *problems of authentication* and its tradeoff with other computational operational aspects. The author has used elliptical curve cryptography for this purpose. Kong et al. [23] have presented an approach to protect *physical layer security*. The authors have presented a key generation that is carried out on the basis of various responses of impulse. The study has presented a mechanism in order to resist the eavesdropping as well as it can also improvise the secret key generation. Poongodi et al. [24] have presented solution against *selective packet dropping* intrusion in adhoc network. The study has constructed a lightweight protocol along with digital signature in order to identify the malicious nodes. Luong et al. [25] have presented a review work to emphasize about the cost modeling practices adopted towards securing wireless network in presence of majority of the fatal attacks. Umar et al. [26] have discussed about the *security problems connected with using cross layer* approach in sensor network. The authors have used fuzzy logic and trust based cross layer protocol in order to address this problem. The work has been carried out using simulation based approach. Wang et al. [27] have addressed the problem of *eavesdropping* where the solution has been presented using game theory. The work is especially focused on physical layer security where an optimal cost model has been presented for this purpose. The study also used enhanced optimization on the basis of simulated annealing. The work of Zhu et al. [28] has also emphasized on reviewing approaches towards improving *physical layer security*. Pu and Lim [29] have presented solution against *selective forwarding attack* using an analytical model that uses simulation-based approach. Sen and Madria [30] has used Bayesian network in order to investigate the *intensity of attack* on the basis of the attack graph analysis.

Hence, there are various forms of research-based approaches that emphasizes on securing wireless network using different methodologies and identifying different problems. The next section discusses research problem.

III. RESEARCH PROBLEM

After reviewing the existing system, there are various open end issues observed with respect to the effectiveness of the security approaches in existing system. This sections briefs of the research problem that has been identified and is addressed in proposed system. Following are the identified research problems:

- *Attack-Specific Solution*: Majority or almost all the existing research work carried out towards securing wireless network are developed to mitigate specific form of attack e.g. jamming attack. Unfortunately, these kinds of solutions are not applicable when the adversarial scenario is changed. Therefore, there is a need to develop a security solution that can address maximum lethal adversaries.
- *Less focus on Responsible Parameters*: In order to develop a robust security model, it is necessary to identify all the extrinsic and intrinsic parameters that are responsible for intrusion. Extrinsic factors may involve deployment scenario of nodes, density, handling management of peak traffic condition. Intrinsic factors may involve buffer availability, processing capability of security protocols, and response time of security protocols. Until and unless these parameters are not considered, effective security solution cannot be developed.
- *Extensive use of Public Key Cryptography*: Adoption of public key cryptography is the best solution towards securing resource-constrained wireless devices. However, they also have pitfalls about generation of keys as well as iterative process of different algorithm to generate security token. Memory management is another bigger issue for the nodes that are in verge of battery saturation state. Existing approaches are required to address these problems which are not found to be carried out.
- *Encryption Mechanism with less Effectiveness*: Any encryption mechanism will consists of iterative steps as well as dependencies of buffer to store the key. Existing approaches uses encryption approach whose decryption steps are just the reverse of it. Unfortunately, such operations can never lead to an effective trapdoor function without which it is not possible to ensure forward and backward secrecy. Hence, existing approaches either focuses on forward or focuses on backward secrecy, which cannot fulfill the full-fledge secure communication in presence of dynamic attacks.
- *Adherence to Security Standard*: Majority of the existing approaches has focused on only any one of security standard e.g. privacy, confidentiality, non-repudiation, integrity, availability, maintainability etc. Although, it is not feasible to implement all of them, but there should be an attempt to include as many of them as possible. Unfortunately, existing approaches has specific focus on implementation which cannot ensure all around security when exposed to highly vulnerable threat in wireless network of any variants.

All the above mentioned problems are addressed in proposed system in order to offer a better solution. The next section discusses about the proposed solution.

IV. RESEARCH METHODOLOGY

This part of the research work is an extension of our prior implementation [31]. The prior implementation has focused on implementing finite field encryption and securing clustering operation while this part of the study is mainly focused on offering data security as well as node anonymity. The prime objective of proposed study is to offer maximum security while transmitting the data over vulnerable wireless network using enhanced public key encryption over finite field.

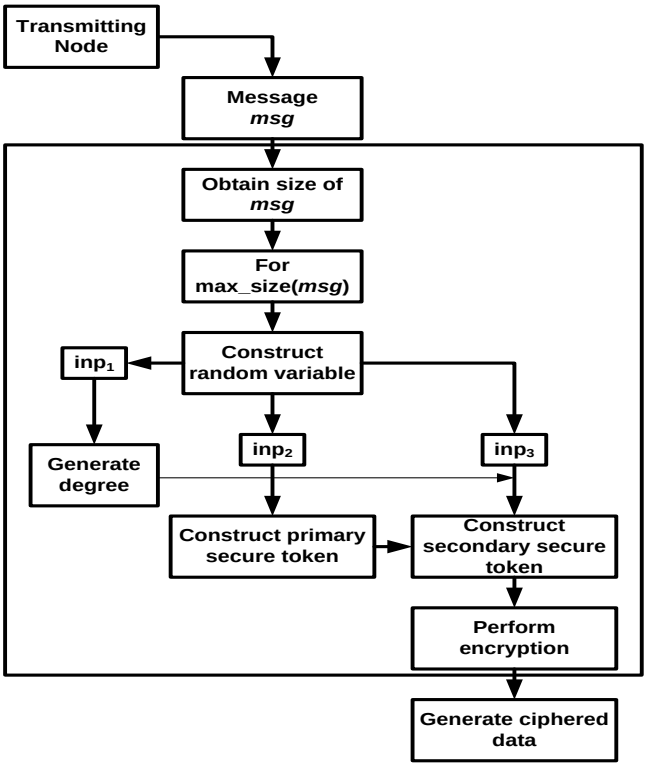

Figure 1 Proposed Architecture

According to the proposed architecture (Fig.1), the proposed system offers multiple layer of security to the message being forwarded by the transmitting device in wireless network. Different from existing public key encryption, the proposed system extracts the size of the message for constructing various multiple smaller version of random variables which are basically random positive integer forms giving rise to combination of three different inputs which are inter-dependent on each other in the form of generation of degree, primary, and secondary toke which are finally used for ciphering the message being forwarded. The contribution of this analytical method is that it not only offers data security but also ensures that no private information about the active communicating nodes are subjected to illegitimate disclosure in the wireless network. With a very simple amendment in public key encryption, proposed system can carry out this operation towards ensuring maximum security.

V. ALGORITHM IMPLEMENTATION

The complete algorithm is design on the basis of public key encryption that is formulated on the basis of algebraic structure considering the finite field. The development of this algorithm is carried out in such a way that it can be used for multiple purposes over the operation to be carried out in security system. The core algorithm developed for this purpose is as shown below:

Algorithm for Ciphering Data

Input: n (number of node)

Output: α (encrypted data)

Start

1. init n
2. *Construct* msg
3. *generate* deg→f_1(inp$_1$)
4. α_1→f_2(dA, inp$_1$)
5. [A, C]→f_3(inp$_2$) -primary security token
6. α→f_4(inp$_3$) -secondary security token

End

The algorithm takes the input of all the number of nodes *n* which after processing yields an outcome of encrypted data *α* (Line-1). The next part of the proposed algorithm is to construct a message in order to carry out transmission (Line-2). Further the algorithm extracts the length of this message and stores it in variable *q*. The next part of the algorithm is about applying a function f_1(x) which takes multiple inputs on the basis of various ranges of prime numbers. This function basically takes two integers and a prime number and computes the degree *deg* which is basically in the form of positive integer. The next part of the algorithmic implementation is about another function f_2(x) that carry out scalar multiplication operation for two input argument i.e. dA and inp$_1$ (Line-4). Basically, the first input argument dA which is a matrix to generate random integer while the second input argument inp$_1$ is same as used in previous line of algorithmic execution. The outcome of this function is α_1 is basically a vector of integer type that represents a point over the algebraic structure while the system makes use of the multiplication of fast integers. It should be noted that applying the two functions f_1(x) and f_2(x) is the novel step carried out in order to amend the conventional mechanism to carry out encryption using public key cryptography. The prime purpose of performing these two steps are mainly to construct a trap-door function in order to offer better control of access policy as well as adherence to maximum security standard (e.g. non-repudiation, confidentiality, and integrity). The non-repudiation will mean non-deniability of service where the user node cannot deny any request from any node; however, while doing so, it will perform randomization of the primary input in such a way using Line-3 and Line-4 that it is nearly impossible to even identify the source of this execution. Hence, non-repudiation as well as confidentiality is maintained at a same time. While it should be noted that this process also constructs a highly comprehensive form of encoding mechanism where indexing is offered for all the data that are required to be encrypted. The generated degree as well as prime numbers are ultimately is in the form of α_1 which can be also consider as a security token. The novelty of this part of the study implementation is that existing public key encryption offers generation of multiple security key where there are chances that atleast one of the secret key will be compromised by any form of attacker. This probability of compromization is mitigated by generating one best secret key only. Once this secret key is used, it will be of no use for any user as well as the newly generated secret key will have no mapping relation with the previous one. Hence, no possibility of even guessing attack could be also successful.

The next part of the implementation is about applying encryption using a function f_3(x) which takes an input of inp$_2$ (Line-5). The function basically performs fast exponentiation method considering two positive integers. According to this operation, the encryption begins with factor *a* (where *a* is one positive integer). Therefore, the output argument A will mean the fast exponentiation method applied over positive integers while the other output argument C will represent modulus of the fast exponentiation method with different input arguments of positive integer. *A* closer look into this part of implementation will show that a combination of A and C will give the overall encrypted value which is stored in matrix whereas the contents of *A* are never equal to C. At the same time, the dependencies of the input arguments for generating value of A as well as C are very much different. Therefore, if any one of them is compromised, attacker will have never an access to the original algorithm structure. Finally, the algorithm carries out ultimate step of security incorporation by constructing a function f_4(x) (Line-6). This function is responsible for generation of a secondary security token α considering the input argument inp$_3$ which consists of i) message *msg* that is obtained from the prior steps of algorithm, ii) a matrix consisting of all the bits of length of message msg, iii) dA, iv) and v) degree *deg*. The operation of this function f_4(x) is carried out in considering following steps.

The algorithm applies fast exponentiation method just like it was carried out in prior steps over similar input arguments of positive integers. The next step will be to carry out integer modulus over other two positive integers, which is further subjected to modulus operation in order to yield the final security token. By this step, the algorithm accomplishes the complete steps of encryption. However, the most interesting part of this algorithm is the mechanism that it applies in order to perform authentication. Different from existing public encryption algorithm, the proposed system doesn't retrace the steps of algorithm to perform decryption. In order to offer a better form of trapdoor function, the proposed system uses very different and multiple parameters used in all prior steps of encryption and secure token generation. Interestingly, it is never feasible to perform extraction of all this input argument to perform validation as all the processing of this input arguments are carried out by different process. Therefore, the proposed algorithm can be claimed to offer better control of illegitimate access over the encrypted data. While assuming that there has been an act of compromise in the network, the algorithm doesn't offer any form of access in the encrypted message as the final validation doesn't carry any input of message information and hence, better data integrity can be claimed.

VI. RESULT ANALYSIS

The proposed system is meant to offer maximal security performance using lightweight public encryption approach. scripted in MATLAB, the analysis is carried out considering 500 wireless node working on standard IEEE 802.11 over 1000 simulation round. The overall data of 2000 bytes has been used for analysis that is further compared with existing public key encryption methods e.g. Elliptical Curve Encryption, Rivest-Shamir Algorithm, and Elgamal Signature Algorithm. For this purpose the analysis of the study is carried out considering three factors as follows:

A. Analysis of Data Forwarding Performance

As the proposed system carry out encryption mechanism, it is essential to find out if there is any potential influence of encryption over the data forwarding process in wireless networks. So, it is assessed using performance parameters of packet delivery ratio, delay, and energy consumption as they are prominent parameters getting affected during security operation carried out in wireless networks.

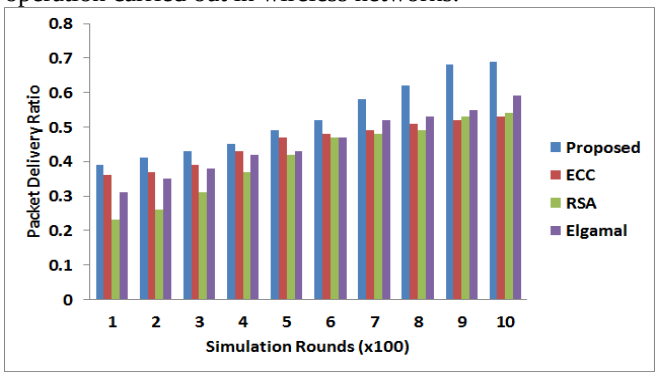

Figure 2 Comparative Analysis of Packet Delivery Ratio

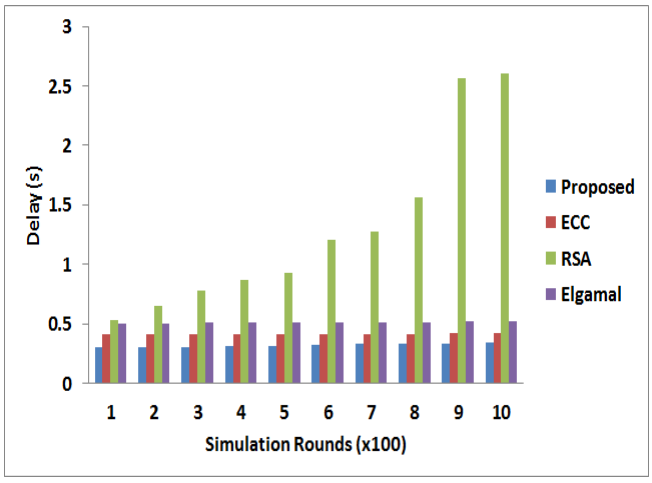

Figure 3 Comparative Analysis of Delay

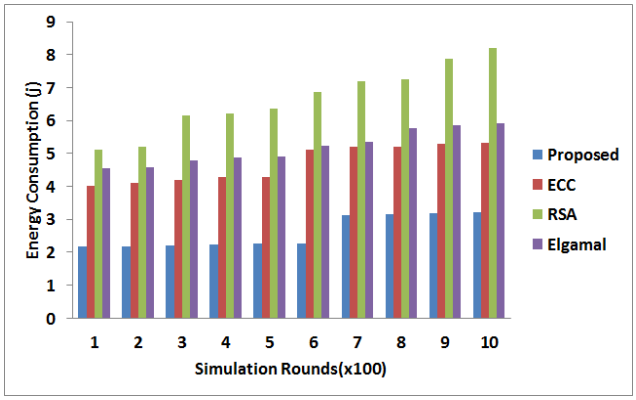

Figure 4 Comparative Analysis of Energy Consumption

The outcome shown from Fig.2 to Fig.4 exhibits that proposed system offer better packet delivery ratio, reduced delay, and reduced energy consumption in comparison with existing system. The prime reason behind packet delivery ratio performance (Fig.2) is that RSA algorithm has bigger key size which limits down the data forwarding process. Elgamal signature performs better than RSA as the dependable variable used for this purpose are much reduced in size which results in smaller key size. However, its validation approach using complex steps and offers multiple dependencies is something that makes ECC better than it. For similar reason, delay performance (Fig.3) can be considered. RSA offers much complexity while generated keys of Elgamal signature are too big sometimes. The data that is used for ciphering in Elgamal signature is double the size of that used in RSA which results in nearly similar performance with RSA. Similarly, the prime causes of energy dissipation are – the entire existing algorithm has sophisticated stages of encryption with larger key size except ECC. Even in ECC, generation of private key is an iterative process. All these are devoid in proposed system that offers more progressive operation with reduced dependencies of abundant complex set of operation. This results in better energy consumption for proposed system (Fig.4).

B. Analysis of Algorithm Complexity

Referring to Fig.5, the algorithm complexity is assessed with respect to algorithm processing time which shows that proposed system offers much faster encryption time as compared to ECC and Elgamal approach. RSA offers too many complexities and hence it is not recommend to be used in wireless nodes.

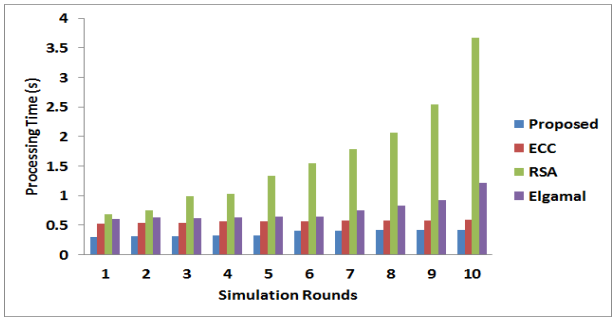

Figure 5 Comparative Analysis of Processing Time

C. Analysis of Security Strength

A closer look at proposed system will show that it is robust trapdoor function where retracing is an impossible for any attacker without consuming massive amount of resources. Hence, various attacks e.g. wormhole attack, Sybil attack, man-in-middle attack, key-based attack can be resisted using this technique over any wireless network. Apart from this, the proposed system offer multiple level of encryption which ensures that non-breakability of ciphered message by any attacker without compromising the entire network system at that instance of time, which is something impossible to attain. Therefore, the proposed system offers maximum security over wireless network.

VII. CONCLUSION

This paper has discussed about a robust modeling that is capable of enhancing the security feature in wireless network. The prime contribution of this paper are as follows: i) it introduces an enhanced public key cryptosystem where using less number of non-iterative operation, maximum security is achieved, ii) an efficient trapdoor function is developed here which offers both forward and backward secrecy in presence of vulnerable situation, iii) the modeling is carried out in highly optimized manner without in inclusion of any sophisticated metrics or approaches, iv) the proposed system is resistive against maximum forms of attack in wireless network, v) the proposed algorithm also maintain a good balance between security features and communication performance.

REFERENCES

1. Anderson, John E., and Paul H. Schwager. "SME adoption of wireless LAN technology: applying the UTAUT model." In Proceedings of the 7th annual conference of the southern association for information systems, vol. 7, pp. 39-43. 2004.
2. Lewis, Daniel E. "Multi-level encryption access point for wireless network." U.S. Patent 6,526,506, issued February 25, 2003.
3. Haleem, Mohamed, Chetan Mathur, Rajarathnam Chandramouli, and Koduvayoor Subbalakshmi. "Opportunistic encryption: A trade-off between security and throughput in wireless networks." IEEE Transactions on Dependable and secure computing 4, no. 4 (2007): 313-324.
4. Frank, Ed H., and Richard Martin. "Method and system for providing multiple encryption in a multi-band multi-protocol hybrid wired/wireless network." U.S. Patent 8,942,375, issued January 27, 2015.
5. Fan, Roderic C., Anil Tiwari, and Ramakrishna Tumuluri. "Wireless device to network server encryption." U.S. Patent 7,983,419, issued July 19, 2011.
6. Boyle, D., and T. Newe. "Security protocols for use with wireless sensor networks: A survey of security architectures." In 2007 Third International Conference on Wireless and Mobile Communications (ICWMC'07), pp. 54-54. IEEE, 2007.
7. Yang, Jie, Yingying Chen, Wade Trappe, and Jerry Cheng. "Detection and localization of multiple spoofing attackers in wireless networks." IEEE Transactions on Parallel and Distributed systems 24, no. 1 (2012): 44-58.
8. Liu, Hongbo, Zhenhua Liu, Yingying Chen, and Wenyuan Xu. "Localizing multiple jamming attackers in wireless networks." In 2011 31st International Conference on Distributed Computing Systems, pp. 517-528. IEEE, 2011.
9. Potlapally, Nachiketh R., Srivaths Ravi, Anand Raghunathan, and Ganesh Lakshminarayana. "Optimizing public-key encryption for wireless clients." In 2002 IEEE International Conference on Communications. Conference Proceedings. ICC 2002 (Cat. No. 02CH37333), vol. 2, pp. 1050-1056. IEEE, 2002.
10. Tejashwini, N., DR Shashi Kumar, and K. Satyanarayana Reddy. "Evolution of Cryptographic Algorithm for Resource Constrained Wireless Networks: An Investigation Approach." Evolution 7, no. 14 (2018).
11. Nguyen, Van-Linh, Po-Ching Lin, and Ren-Hung Hwang. "Energy Depletion Attacks in Low Power Wireless Networks." IEEE Access 7 (2019): 51915-51932.
12. Ding, Xiaojin, Yulong Zou, Fei Ding, Dengyin Zhang, and Gengxin Zhang. "Opportunistic Relaying Against Eavesdropping for Internet-of-Things: A Security-Reliability Tradeoff Perspective." IEEE Internet of Things Journal 6, no. 5 (2019): 8727-8738.
13. Aliady, Wateen A., and Saad A. Al-Ahmadi. "Energy Preserving Secure Measure Against Wormhole Attack in Wireless Sensor Networks." IEEE Access 7 (2019): 84132-84141.
14. Han, Weihong, Zhihong Tian, Zizhong Huang, Dongqiu Huang, and Yan Jia. "Quantitative Assessment of Wireless Connected Intelligent Robot Swarms Network Security Situation." IEEE Access 7 (2019): 134293-134300.
15. Tsiota, Anastasia, Dionysis Xenakis, Nikos Passas, and Lazaros Merakos. "On Jamming and Black Hole Attacks in Heterogeneous Wireless Networks." IEEE Transactions on Vehicular Technology 68, no. 11 (2019): 10761-10774.
16. Vashist, Abhishek, Andrew Keats, Sai Manoj Pudukotai Dinakarrao, and Amlan Ganguly. "Securing a Wireless Network-on-Chip Against Jamming-Based Denial-of-Service and Eavesdropping Attacks." IEEE Transactions on Very Large Scale Integration (VLSI) Systems 27, no. 12 (2019): 2781-2791.
17. Yun, Jusik, Sunho Seo, and Jong-Moon Chung. "Centralized trust-based secure routing in wireless networks." IEEE Wireless Communications Letters 7, no. 6 (2018): 1066-1069.
18. Fang, Dongfeng, Yi Qian, and Rose Qingyang Hu. "Security for 5G mobile wireless networks." IEEE Access 6 (2017): 4850-4874.
19. Guan, Yanpeng, and Xiaohua Ge. "Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks." IEEE Transactions on Signal and Information Processing over Networks 4, no. 1 (2017): 48-59.
20. Guan, Yanpeng, and Xiaohua Ge. "Distributed secure estimation over wireless sensor networks against random multichannel jamming attacks." IEEE Access 5 (2017): 10858-10870.
21. Heo, Jeongyoon, Jung-Jun Kim, Jeongyeup Paek, and Saewoong Bahk. "Mitigating stealthy jamming attacks in low-power and lossy wireless networks." Journal of Communications and Networks 20, no. 2 (2018): 219-230.
22. Ever, Yoney Kirsal. "Secure-anonymous user Authentication scheme for e-healthcare application using wireless medical sensor networks." IEEE systems journal 13, no. 1 (2018): 456-467.
23. Kong, Yuanyuan, Bin Lyu, Feng Chen, and Zhen Yang. "The security network coding system with physical layer key generation in two-way relay networks." IEEE Access 6 (2018): 40673-40681.
24. Poongodi, T., Mohammed S. Khan, Rizwan Patan, Amir H. Gandomi, and Balamurugan Balusamy. "Robust Defense Scheme Against Selective Drop Attack in Wireless Ad Hoc Networks." IEEE access 7 (2019): 18409-18419.
25. Luong, Nguyen Cong, Dinh Thai Hoang, Ping Wang, Dusit Niyato, and Zhu Han. "Applications of economic and pricing models for wireless network security: A survey." IEEE Communications Surveys & Tutorials 19, no. 4 (2017): 2735-2767.
26. Umar, Idris Abubakar, Zurina Mohd Hanapi, Aduwati Sali, and Zuriati A. Zulkarnain. "TruFiX: A configurable trust-based cross-layer protocol for wireless sensor networks." IEEE Access 5 (2017): 2550-2562.
27. Wang, Kun, Li Yuan, Toshiaki Miyazaki, Deze Zeng, Song Guo, and Yanfei Sun. "Strategic antieavesdropping game for physical layer security in wireless cooperative networks." IEEE Transactions on Vehicular Technology 66, no. 10 (2017): 9448-9457.
28. Zhu, Jia, Yulong Zou, and Baoyu Zheng. "Physical-layer security and reliability challenges for industrial wireless sensor networks." IEEE access 5 (2017): 5313-5320.
29. Pu, Cong, and Sunho Lim. "A light-weight countermeasure to forwarding misbehavior in wireless sensor networks: design, analysis, and evaluation." IEEE Systems Journal 12, no. 1 (2016): 834-842.
30. Sen, Amartya, and Sanjay Madria. "Risk assessment in a sensor cloud framework using attack graphs." IEEE Transactions on Services Computing 10, no. 6 (2016): 942-955.
31. Tejashwini, N., DR Shashi Kumar, and K. Satyanarayan Reddy. "Novel Filtering-Based Approach Using Fuzzy Logic for Prevention of Adversaries in Sensory Application." In Computer Science On-line Conference, pp. 1-10. Springer, Cham, 2019.

AUTHORS DETAIL

	**Tejashwini N,** She has completed her B.E from SVCE, Bengaluru Karnataka and M.Tech is from Dr. AIT, Bengaluru, Karanataka, She having six years of teaching and research experience in respective engineering colleges under Visvesvaraya Technological University, Belagavi, Karnataka, India. Her interest includes Digital image communication, Wireless communication, Wireless sensor network and Operating system. Currently she is pursuing her research for PhD under Visvesvaraya Technological University, Belagavi, Karnataka. She has published her work in various international conferences and journals.
	**Dr. D R Shashi Kumar,** Currentlly working as a Professor and HOD, Department of CSE, Cambridge Institute of Technology, Bengaluru, Karnataka, India. He has more than 29 working in various capacities. He has More than 20 Research Papers (National and International) in his credit and has chaired national and international conferences. He has published 10 research papers in refereed International Technical Journals with good Impact factor. His research interest area is Digital Image Processing, Computer Networks-Specialization Microprocessors, Data Mining, and Neural Networks.
	**Dr. K Satyanarayana Reddy**, Currentlly working as a Professor and HOD, Department of ISE, Cambridge Institute of Technology, Bengaluru, Karnataka, India. He has more than 25 years of experience in academics in the field of Computer Science. He has more than 25 Research Papers (National and International) in his credit and has chaired national and international conferences. Delivered Keynote address in few national level conferences. His area of interst is Artificial Intelligence and Robotics, Computer Networks, Data Communications, Software Engineering, Theoretical Computer Science, Wireless Sensor Networks.