International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-3, January 2020

Trust and Cryptography Centered Privileged Routing Providing Reliability for WSN Considering Dos Attack Designed for AMI of Smart Grid

Priyanka D. Halle, Shiyamala S.

Abstract*: Sheltered communication is a precise significant concern in any kind of network. This research focuses on secure and reliable wireless message arrangement. Through relating trust based and cryptography based approach we can progress wireless communication security and reliability effectually of Advanced Metering Infrastructure. Wireless Sensor Network used as a communiqué arrangement for AMI.Nodes(Sensors) are employed intended for a Home Area Network around 10-60.The performance of security and reliability calculated through energy depletion, delay, packet transfer ratio or packet delivery ratio (PDR),throughput and overhead of the sensor nodes. Diverse categories of attacks arises on wireless communication infrastructure. This research deliberated Denial of Service (DoS) type attack. Through linking Elliptic Curve Cryptography (ECC) for secure routing and authenticated anonymous secure routing (AASR) for reliable route routing tries to improve reliability and security of wireless communication infrastructure of AMI using NS2(Network Simulator2) simulation platform. Operative routing delivers radical change in enactment of wireless communication infrastructure. Proposed AASR protocol and ECC protocol admirably delivers virtuous results compared to surviving protocols.

Keywords: **AASR, ECC, WSN, DoS attack, routing.**

I. INTRODUCTION

Smart Grid (SG) tried to improve the performance of electricity sector by providing secure Advanced Metering Infrastructure (AMI) element. The different types of threats degrades the performance of SG and AMI habitually Cyber Attacks and Physical attacks. These kind of attacks disturbs the system and electricity sector degrades the performance [1].Electricity is an elementary constituent in every field and social development.

Revised Manuscript Received on January 30, 2020.
***** Correspondence Author
Priyanka D. Halle*, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamilnadu, India
Dr. Shiyamala S., Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamilnadu, India

The demand of electricity rapidly increases day by day.SG and AMI tries to provide this kind of demand smartly. However different kinds of threats disturbs the AMI and SG.Many researchers are working on the same problem still problems not solved yet. Smart Meter(SM) is a basic part of AMI.It ropes electric load calculating, anomaly finding and request response program growth [2].AMI infrastructure management supports smart and secure wireless communication infrastructure and communication technologies. It supports bidirectional communication infrastructure. It is one of the superlative feature of AMI.Electricity sector energies through different process like substation, generation, distribution. In every stage different threats provide challenging work to the electricity sector. On the other hand AMI energies through the different stages. Bidirectional communiqué helps to save electricity. It will possible through wireless communication infrastructure [3].This research considered wireless sensor Network (WSN) for communiqué substructure designed for AMI. Transmitter authentication and privacy-preserving of user's data are the very basic foremost security difficulties in SG communication. The electricity sectors are going to work together with information technicians to embrace different cyber security techniques for the AMI and SG to preserve reliability. Security enhances reliability [4].Acquiring a secure communiqué means tapping the antagonist in a detrimental station with deference to the authentic representative. Secure communication usually adopted using combining traditional and modern cryptographic techniques to encrypt and decrypt communication content [5]. AMI goes to the customer and the distribution areas and it is accountable for gathering, calculating and examining electricity.MDMS is a part of AMI headend and it is a sever of AMI.The different kinds of bouts mainly happens on meter data management system. And it disturbs the arrangement. Security is a big issue of every wireless communication technologies. It's a challenging work for every researcher to provide secure wireless communication technologies to AMI.Around three basic key elements of security 1.Confidentiality 2.Integrity 3.Availability [6].

For WSN confidentiality is a key element for security purpose. And many researchers are tried to provide security for WSN in terms of confidentiality by providing different algorithms and protocols.

Still WSN faces different kinds of attacks on confidentiality [7]. The IEEE 802.16e standards had developed different security protocols for WiMAX. These protocols combines different security algorithms and protocols, techniques for security development. Still it undergoes different kinds of attack [8].Hybrid DoS Attack many times occurred in WSN.For early detection of same kind of attack trust based energy consumption node

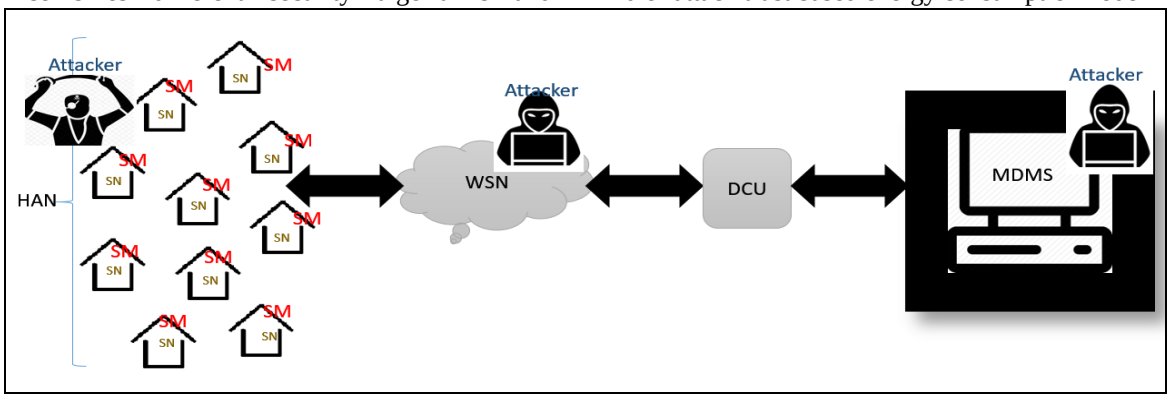


Fig. 1. Architecture of AMI(SM-Smart Meter, SN-Smart Node, DCU-Data Control Unit)

Table- I: Fundamental elements of Security for Wireless Networks and their proposed solution considering different attacks

Ref. No.	Key element considered for security	Methodology/Algorithm/Protocol considered	Considered Network	Considered Attack
16.	Confidentiality, Integrity and Availability	Advanced control algorithms, web protocols, routing protocols	WSN	massive malicious attacks, deliberate attacks, Internal and external attacks, active, passive, layered attacks
20.	Confidentiality, integrity	Robust stream cipher		key recovery attacks
21.	Availability	HWMP, the LA-HWMP, colony algorithm and simulated annealing (ACA-SA)		
22.	confidentiality, integrity and availability	Dynamic key management algorithm		Black hole attacks

Table- II:Proposed work consideration parameters

Design and Evaluation Recent Security Methods			
Case - A	**Random Deployment of AMI**	Smart meter nodes	10-60
		Data Collector nodes	2
		Utility node	1
		Wireless Communication	Smart Meter Nodes to Data Collector Nodes
		Wired Communication	Data Collector to Utility Node
		Malicious Attackers	10 %
		MAC	802.11
		Routing Protocols	AODV, DSDV, AASR [1] Cryptography based and TERP [2] Trust Based
		Simulation Time	100 seconds
		Performance Metrics	Throughput vs. Number of nodes
			Delay vs. Number of nodes
			PDR vs. Number of nodes
			Overhead vs. Number of nodes
			Packet loss vs. Number of Nodes
Case - B	**Grid Deployment of AMI**	Smart meter nodes	25, 36, 49
		Data Collector nodes	2
		Utility node	1
		Wireless Communication	Smart Meter Nodes to Data Collector Nodes
		Wired Communication	Data Collector to Utility Node
		Malicious Attackers	10 %
		MAC	802.11
		Routing Protocols	AODV and DSDV (Proactive and Reactive)
		Simulation Time	100 seconds
		Performance Metrics	Throughput vs. Number of nodes

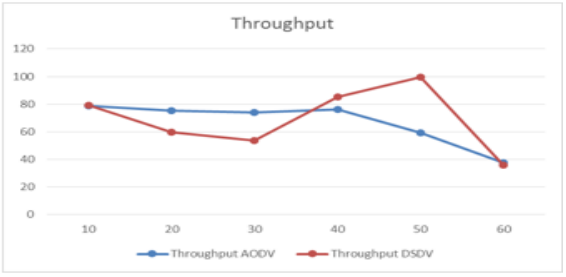
			Delay vs. Number of nodes
			PDR vs. Number of nodes
			Overhead vs. Number of nodes
			Packet loss vs. Number of Nodes

Table- III: Proposed work consideration parameters with results (VH-Very High, VL-Very Low)

Protocol/Parameters	Throughput	Delay	Overhead	PDR	Energy consumption
AODV					
DSDV					
AASR			VL		
TERP	VH	VL	VL	VH	VL

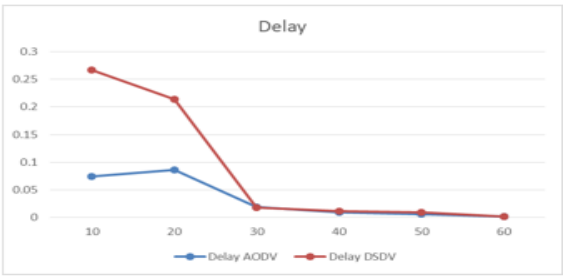
Throughput

NODES	AODV	DSDV
10	78.58	79.4
20	75.32	59.62
30	74.18	53.4
40	76.21	85.3
50	59.07	99.43
60	37.44	35.71



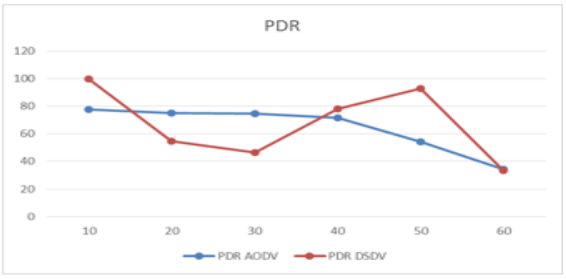
Delay

NODES	AODV	DSDV
10	0.07408	0.2667
20	0.08628	0.2142
30	0.01885	0.018
40	0.009493	0.01137
50	0.006316	0.0093
60	0.00178	0.001086



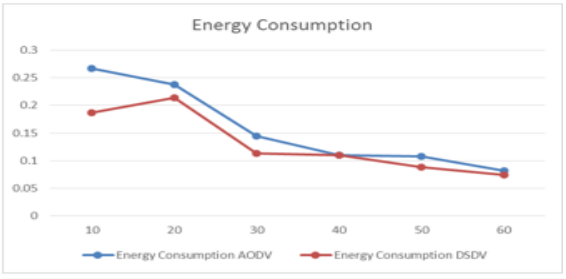
PDR

NODES	AODV	DSDV
10	77.79	100
20	74.96	54.85
30	74.62	46.353
40	71.51	78.26
50	54.05	92.69
60	34.45	33.33



Energy Consumption

NODES	AODV	DSDV
10	0.2673	0.1871
20	0.238	0.2142
30	0.1451	0.1129
40	0.1097	0.1097
50	0.1078	0.08823
60	0.08196	0.07377



Overhead

NODES	AODV	DSDV
10	0.211	0.113
20	0.472	0.333
30	0.589	1.2
40	1.051	1.295
50	1.478	1.384
60	2.426	4.472

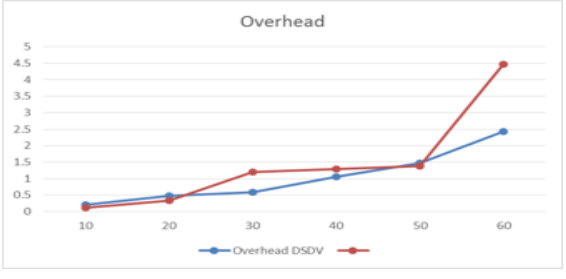


Fig. 2.Simulation results AODV and DSDV

technique used. It combines energy consumption algorithm and energy trust algorithm and efficiently it gives result. Energy consumption design helps to estimate security state of nodes.WSN routines radio communication for wireless communication and ultimately it provides vulnerabilities. Eventually DoS attacks arises further on WSN infrastructure [9].Packet Delivery Ratio, Throughput, node average energy consumption try to provide security for WSN considering routing. Energy Optimized Secure Routing rectify malicious nodes and improve security of AMI [10].

II. AMI ARCHITECTURE

In AMI architecture, secure communication structure is crucial constituent of AMI.By providing secure communication structure and cyber security we can develop the security of AMI.WSN is one of the superlative prime for wireless communication structure of AMI.The many researchers are vigorously doing research on security of WSN.Energy consumption, throughput, delay and security these are some major issues of WSN.In WSN selection of secure routing protocol is a challenging work. DoS attack is a one type of threat of WSN [11].For every wireless network, it has a feature about secure routing protocol. So that the wireless network will give good performance.Data integrity and data confidentiality

Protects the wireless networks from the different attacks [12].WSN appearances different problems such as documents crash, signal weakening, energy deficiency, mobility and spiteful bouts.Considereing these problems researchers are going to solve the problems by providing security in terms of CIA model[13].Figure 1 contributes in ephemeral impression of AMI architecture and its main components. The AMI architecture gives overall idea about this paper. In this paper researcher are tried to give strong wireless communication infrastructure by providing

Throughput

NODES	AODV	DSDV	Cryptography
10	78.58	79.4	81.72
20	75.32	59.62	80.97
30	74.18	53.4	78.23
40	76.21	85.3	78.11
50	59.07	99.43	63.5
60	37.44	35.71	40.25

Delay

NODES	AODV	DSDV	Cryptography
10	0.07408	0.2667	0.08816
20	0.08628	0.2142	0.07568
30	0.01885	0.018	0.02269
40	0.009493	0.01137	0.01211
50	0.006316	0.0093	0.00822
60	0.00178	0.001086	0.00281

PDR

NODES	AODV	DSDV	Cryptography
10	77.79	100	90.22
20	74.96	54.85	89.95
30	74.62	46.353	87.26
40	71.51	78.26	86.99
50	54.05	92.69	66.58
60	34.45	33.33	47.024

Overhead

NODES	AODV	DSDV	Cryptography
10	0.211	0.113	0.255
20	0.472	0.333	0.674
30	0.589	1.2	0.674
40	1.051	1.295	1.34
50	1.478	1.384	1.92
60	2.426	4.472	3.82

Energy Consumption

NODES	AODV	DSDV	Cryptography
10	0.2673	0.1871	0.2585
20	0.238	0.2142	0.2469
30	0.1451	0.1129	0.1301
40	0.1097	0.1097	0.09475
50	0.1078	0.08823	0.09284
60	0.08196	0.07377	0.06696

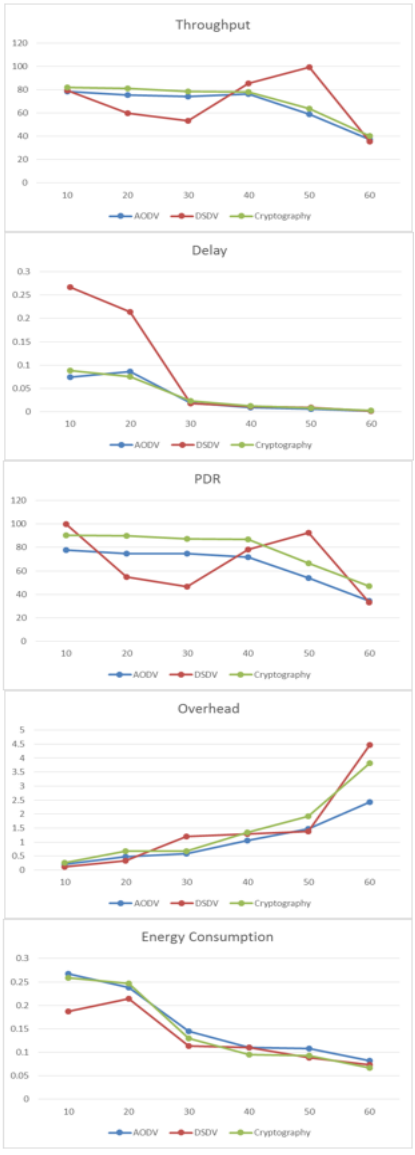


Fig. 3.Simulation results AODV, DSDV and cryptography based approach

WSN.The different kinds of attacks occurs on the different area of WSN.By considering different parts of WSN the researchers are tried to provide security still it faces problem of security but as compared to other communication infrastructure WSN is more reliable and secure. Broadcast communication constantly desired by WSN subsequently attacker can construe the information and bothers the system. WSN is a set of sensor nodes. Miscellany of routing protocol for WSN is an inspiring task because the without routing WSN will not enhance the security [14].Power routing (PR), Rumor routing (RR), Geographic routing (GR), Opportunistic routing (OR) habitually favored for WSN.By combing GR and OR researcher's deliver superlative opportunity for WSN routing[15]. In SG progressive Information and Communication Technologies (ICT) provides various functionalities.WSN constantly keeps smart ICTs.Smart Metering infrastructure similar to SN, SM, WSN, DCU and MDMS allows directly collaboration among the energy utility and patrons due to bidirectional communication [16].Ultimately SG provides smart electricity market with social development.

A. Routing

Secure routing selection is a fascinating work for AMI.Routing protocol provides superlative path to transfer sensitive data from one place to another place. Proactive and reactive routing protocols provides good performance still it faces many issues related to the security. Hybrid routing protocols having excellent performance. Numerous researcher's try to combine proactive and reactive protocols for numerous performance characteristics.

Throughput

NODES	AODV	DSDV	Cryptography	Trust based
10	78.58	79.4	81.72	83.82
20	75.32	59.62	80.97	82.85
30	74.18	53.4	78.23	80.92
40	76.21	85.3	78.11	80.49
50	59.07	99.43	63.5	66.45
60	37.44	35.71	40.25	42.12

Delay

NODES	AODV	DSDV	Cryptography	Trust based
10	0.07408	0.2667	0.08816	0.07408
20	0.08628	0.2142	0.07568	0.07072
30	0.01885	0.018	0.02269	0.01885
40	0.009493	0.01137	0.01211	0.009493
50	0.006316	0.0093	0.00822	0.006316
60	0.00178	0.001086	0.00281	0.001784

PDR

NODES	AODV	DSDV	Cryptography	Trust based
10	77.79	100	90.22	94.366
20	74.96	54.85	89.95	94.45
30	74.62	46.353	87.26	91.48
40	71.51	78.26	86.99	92.15
50	54.05	92.69	66.58	70.76
60	34.45	33.33	47.024	51.21

Overhead

NODES	AODV	DSDV	Cryptography	Trust based
10	0.211	0.113	0.255	0.279
20	0.472	0.333	0.674	0.524
30	0.589	1.2	0.674	0.615
40	1.051	1.295	1.34	1.132
50	1.478	1.384	1.92	1.601
60	2.426	4.472	3.82	2.76

Energy consumption

NODES	AODV	DSDV	Cryptography	Trust based
10	0.2673	0.1871	0.2585	0.2614
20	0.238	0.2142	0.2469	0.228
30	0.1451	0.1129	0.1301	0.1351
40	0.1097	0.1097	0.09475	0.09975
50	0.1078	0.08823	0.09284	0.09784
60	0.08196	0.07377	0.06696	0.07196

Fig. 4.Simulation results AODV, DSDV, cryptography based approach and trust based approach

It combines good characteristics and features of both still it faces the problems, extremely zone-overlapping amount, unbalanced momentary routing, and dense routing overhead [17].WSN's performance based on routing.WSNs are vulnerable to DoS attacks,sybilattacks,black hole attacks and many more. At the time of selection of routing protocol researcher's has to calculate risk and risk is based on threat and vulnerability factors [18].In WSN SN continuously gather the information in the form of physical quantity and the forward this sensitive data to base station for further processing.SN plays very vital role in wireless communication infrastructure.SN should send secure data. Considering this requirement designer has to choose secure and reliable routing. Due to usage of clustering WSN can improve the performance. It tries to reduce routing overheads and sensor energy consumption [19]. Table 1 delivers different algorithms and protocols considering key elements of security. Packet routing is one of the significant part of AMI network processes. Routing method selection is based on type of communication infrastructure. Voluminous researcher's had chosen different routing protocols and routing algorithms, method based on the communication infrastructure and type of a network. Each routing methods having some advantages and disadvantages consequently combination of them implemented and it gives tremendous advantages to AMI performance [21]. In WSN routing DoS attack try to disturb the network operation .This research considering the DoS attack which is active type of attack. In security policy key management is a very important factor. Broadcast secure authentication protocols supports for key management in WSN.Ultimately three types of key formation protocols used in WSN:-1.Hybrid 2.Probabilistic 3.Deterministic[22].

III. TRUST BASED AND CRYPTOGRAPHY BASED APPROACH FOR SECURITY (PROPOSED WORK)

This research tries to give solution by considering key elements for security of AMI communication infrastructure. The key requirement of AMI systems is the securities from the various attacks are wireless communications such as Wi-fi or WLAN networks. The performance can be calculated of cyber security by taking key elements means CIA model. Which may be vulnerable to wireless security threats during the wireless communications. Thus, we mainly focus on designing the reliable and secure method that achieve satisfy the security requirements as well as improve the QoS performance of routing as compared to the underlying with and without security based routing protocols under the presence of various attacks such as DoS. We considered random deployment and grid deployment for AMI. For the same development of a security is a main issue and that can be accomplished using basic parameters calculation in terms of security of a network 1.Throughput 2.Delay 3.Packet Delivery Ratio (PDR) 4.overhead 5.energy consumption.

AODV and DSDV are elementary routing protocols which couldn't deliver satisfactory results for security. Consequently in this paper researcher again tried to combine trust based (TERP) approach and cryptography based (AASR) methodology to develop the recital of security and ultimately it improves the performance. Still somehow it provides less security because of more vulnerabilities and more threats of wireless communication infrastructure. Combining cryptography based and trust based approach enhanced the security of wireless communication infrastructure still researchers have to do work on security issue foe wireless communication infrastructure for AMI [23][24].Table2 provides information related to proposed work.

Results are simulated using simulation platform NS2.It is one of the best solution for network based parameters analysis.Ananysis results comparatively gives good security. TERP and AASR comparatively enhances the security than AODV and DSDV [23] _ [35].

IV. CONCLUSION

Eventually, coalescing modern cryptography based and trust based protocols tried to deliver worthy security for wireless communication infrastructure which is considered in this research WSN for AMI.Secure routing is a key element of security. Ultimately secure routing provides secure wireless communication. Network Simulator 2 is very good simulation platform for networking purpose. It provided simulation result will help to calculate the performance characteristics. Finally combined solution enhances the results in standings of reducing energy ingesting, increasing quantity, increasing PDR, reducing overhead plus delay.

FUTURE SCOPE

A lot of scientists are working on protection for wireless communiqué arrangement for considering different kinds of attacks. Many of them provided solution combining different types of algorithms, protocols and ultimately it gives virtuous consequences. But still different threats try to destroy wireless communication system. AMI is a part of SG.AMI faces different kinds of vulnerabilities. And so that electricity sector vitiates the performance. Many researchers have to do work on security parameters for routing in WSN.

REFERENCES

1. Abdulrahaman Okino Otuoze, Mohd Wazir Mustafa, Raja Masood Larik, "Review Smart grids security challenges: Classification by sources of threats", Received 24 December 2016; received in revised form 14 August 2017; accepted 5 January 2018.
2. Lulu Wen, Kaile Zhou, Shanlin Yang, Lanlan Lia, "Compression of smart meter big data: A survey", Received 20 January 2017; Received in revised form 29 March 2018; Accepted 30 March 2018.
3. Dariush Abbasinezhad-Mood, Morteza Nikooghadam, "Design of an enhanced message authentication scheme for smart grid and its performance analysis on an ARM Cortex-M3 microcontroller", Available online 5 March 2018.
4. Ulas Baran BALOGLU, Yakup DEMúIR, "Lightweight Privacy-Preserving Data Aggregation Scheme for Smart Grid Metering Infrastructure Protection", 27 April 2018.
5. Mirko Bottarelli, Gregory Epiphaniou, Dhouha Kbaier Ben Ismail, Petros Karadimas, Haider Al-Khateeb, "Physical Characteristics of Wireless Communication Channels for Secret Key Establishment: A Survey of the Research" 1 August 2018.
6. Zakaria El Mrabet, Naima Kaabouch, Hassan El Ghazi, Hamid El Ghazi, "Cyber-security in smart grid: Survey and challenges", Accepted 12 January 2018.

7. Yu Li, Xiaotian Wang, Dae Wook Kim, Junjie Zhang, Rui Dai, " Designing self-destructing wireless sensors with security and performance assurance", Available online 17 May 2018.
8. Prabhat Kumar Panda, Sudipta Chattopadhyay, "A modified PKM environment for the security enhancement of IEEE 802.16e", Received 27 November 2017; Received in revised form 11 May 2018; Accepted 2 June 2018.
9. Xie Jinhui, Tao Yang, Yang Feiyue, Pan Leina, Xu Juan, Hou Yao, "Intrusion Detection System for Hybrid DoS Attacks using Energy Trust in Wireless Sensor Networks",8th International Congress of Information and Communication Technology (ICICT-2018).
10. Tao Yang, Xu Xiangyan, Li Peng, Li Tonghui, Pan Leina, "A secure routing of wireless sensor networks based on trust evaluation model", Tao Yang et al./ Procedia Computer Science 131 (2018) 1156–1163 1157.
11. Sudeep Tanwar, Kenny Thakkar, Ruchi Thakor, and Pradeep Kr Singh, "M-Tesla-Based Security Assessment in Wireless Sensor Network "International Conference on Computational Intelligence and Data Science (ICCIDS 2018).
12. Younes ASIMI, Ahmed ASIMI, Azidine GUEZZAZ, Zakariae TBATOU, " Unpredictable cryptographic primitives for the Robust Wireless Network Security", The 2nd International Workshop on Big Data and Networks Technologies (BDNT 2018).
13. Huafeng Wu, Jiangfeng Xian, Jun Wang, Siddhi Khandge,Prasant Mohapatra, "Missing data recovery using reconstruction in ocean wireless sensor networks", 17 September 2018.
14. Matthew Bradbury, Arshad Jhumka, Matthew Leeke, "Hybrid online protocols for source location privacy in wireless sensor networks", 22 January 2018.
15. Chen Liu , Dingyi Fang , Yue Hu , Shensheng Tang , Dan Xu, Wen Cui , Xiaojiang Chen , Baoying Liu, Guangquan Xu, Hao Chen, "Easy Go: Low-cost and robust geographic opportunistic sensing routing in a strip topology wireless sensor network", Accepted 2 July 2018.
16. M. Faheem, S.B.H. Shah, R.A. Butt, B. Raza, M. Anwar, M.W. Ashraf, Md.A. Ngadi, V.C. Gungor, "Review article Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges", Accepted 10 August 2018.
17. Xueqin Yang, Qiangwei Chen, Chaobo Chen, Jianhua Zhao, "Improved ZRP Routing Protocol Based on Clustering",8th International Congress of Information and Communication Technology (ICICT-2018).
18. Tao Yang, Xu Xiangyang, Li Peng, Li Tonghui, Pan Leina, "A secure routing of wireless sensor networks based on trust evaluation model", 8th International Congress of Information and Communication Technology (ICICT-2018).
19. Sudeep Tanwar, Kenny Thakkar, Ruchi Thakor, and Pradeep Kr Singh, "M-Tesla-Based Security Assessment in Wireless Sensor Network", International Conference on Computational Intelligence and Data Science (ICCIDS 2018).
20. Younes ASIMI, Ahmed ASIMI, Azidine GUEZZAZ, Zakariae TBATOU, "Unpredictable cryptographic primitives for the Robust Wireless Network Security", The 2nd International Workshop on Big Data and Networks Technologies (BDNT 2018).
21. A. Robert singh, D. Devaraj, R. Narmatha Banu, "Genetic algorithm-based optimisation of load-balanced routing for AMI with wireless mesh networks", 1 October 2018.
22. Mohammad Sadegh Yousefpoor, Hamid Barati, "Dynamic key management algorithms in wireless sensor networks: A survey", 19 November 2018.
23. Wei Liu and Ming Yu, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. X, NO. Y, MARCH 2014
24. Jian Shen, Chen Wang, Aniello Castiglione, Dengzhi Liu and Christian Esposito, "Trustworthiness Evaluation-based Routing Protocol for Incompletely Predictable Vehicular Ad hoc Networks", IEEE TRANSACTIONS ON BIG DATA, VOL. X, NO. Y, OCTOBER-NOVEMBER 2017
25. N Chaitanya Kumar, Abdul Basit, Priyadarshi Singh, and V. Ch. Venkaiah, "Lightweight Cryptography for Distributed PKI Based MANETS", International Journal of Computer Networks & Communications (IJCNC) Vol.10, No.2, March 2018, DOI: 10.5121/ijcnc.2018.10207
26. Sree Lekshmi S., Sivraj P. and Sasi K.K., "Selection of Routing Protocols for Advanced Metering Infrastructure", 2016 Intl. Conference on Advances in Computing, Communications and Informatics (ICACCI), Sept. 21-24, 2016, Jaipur, India
27. Yakubu Tsado, Kelum A. A. Gamage, Bamidele Adebisi, David Lund, Khaled M. Rabie
28. And Augustine Ikpehai, "Improving the Reliability of Optimised Link State Routing in a Smart Grid Neighbour Area Network based Wireless Mesh Network Using Multiple Metrics", Energies 2017, 10, 287; doi: 10.3390/en10030287
29. Shunrong Jiang, Student Member, IEEE, Xiaoyan Zhu, Member, IEEE, and Liangmin Wang, Member, IEEE, "An Efficient Anonymous Batch Authentication Scheme Based on HMAC for VANETs" 1524-9050 © 2016 IEEE.
30. Nian Liu, Member, IEEE, Jinshan Chen, Lin Zhu, Jianhua Zhang, Member, IEEE, and Yanling , "A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid" IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 10, OCTOBER 2013
31. Pranjali Deepak Nikam, Vanita Raut, "Improved MANET security using Elliptic Curve Cryptography and EAACK" 2015 International Conference on Computational Intelligence and Communication Networks.
32. Zhexiong Wei, Helen Tang, Member, IEEE, F. Richard Yu, Senior Member, IEEE, Maoyu Wang, and Peter Mason, "Security Enhancements for Mobile Ad Hoc Networks With Trust Management Using Uncertain Reasoning" IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 63, NO. 9, NOVEMBER 2014.
33. Mohamed M.E.A. Mahmoud, Xiaodong Lin, Senior Member, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE, "Secure and Reliable Routing Protocols for Heterogeneous Multi hop Wireless Networks" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO. 4, APRIL 2015.
34. Stylianos Kraounakis, Ioannis N. Demetropoulos, Angelos Michalas, Member, IEEE, Mohammad S. Obaidat, Fellow, IEEE, Panagiotis G. Sarigiannidis, Member, IEEE, and Malamati D. Louta, Senior Member, IEEE, "A Robust Reputation-Based Computational Model for Trust Establishment in Pervasive Systems" IEEE SYSTEMS JOURNAL, VOL. 9, NO. 3, SEPTEMBER 2015
35. Dhanya and Dr.L.Pavithira, "A Secure Cluster based VANET Modelling System with keyed Hash Message Authentication Code", ISSN: 0976-1353 Volume 23 Issue 5 –SEPTEMBER 2016.G. O. Young, "Synthetic structure of industrial plastics (Book style with paper title and editor)," in Plastics, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.

AUTHORS PROFILE

Ms. Priyanka D. Halle, is employed as Assistant Professor in Electronics and Telecommunication Engineering Department, Institute of SKN Sinhgad Institute of Technology & Science, Pune. She is having Teaching Experience of Six years in the engineering field. She is doing PhD in Security for wireless communication at VTU Chennai from Feb. 2017.

S. Shiyamala, received B.E. and M.E. degrees in ECE from PSNACET, Madurai Kamaraj University and RVSCET, Anna University, Chennai in 1995 and 2004, respectively. She received her Ph.D. degree in Information and Communication Engineering in Anna University, Tiruchirappalli. Currently she is working as an Associate professor in the department of ECE, Veltech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai, India