International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

Secure Routing through Refining Reliability for WSN against DoS Attacks using AODSD2V2 Algorithm for AMI

Priyanka D. Halle, Shiyamala S.

Abstract*: Secure and reliable routing expands the performance of wireless communication infrastructure of the Advanced Metering Infrastructure (AMI).This paper tries to deliver reliable routing using combination of AODV(Reactive type protocol) and DSDV(proactive type protocol) protocol considering WSN. Different kinds of Attack annoys the enactment of communication infrastructure of AMI. This paper defends communication infrastructure from DoS (Denial of service) attack. The main aim of this paper try to provide reliable routing with security. Communication infrastructure is a key element of AMI. Providing reliability and security for communication infrastructure we can improve the performance of AMI. Due to this electricity sector can save millions of dollars and we provide social awareness about importance of electricity security or Smart Grid. This paper calculates the security in terms of delay, energy consumption, throughput, PDR (Packet Delivery Ratio) and overhead. By considering these parameters we will calculate Confidentiality, Integrity, Availability and Accountability (non- repudiation). Wireless Sensor Network (WSN) considered for wireless communication infrastructure for the AMI. Sensor nodes are battered for attack. Intended for AODSD2V2 (Ad Hoc on Demand Destination Sequenced Distance Vector Routing Protocol) protects the data packets from malicious nodes and DoS attack. For the WSN network infrastructure two kinds of topologies are considered 1. Random deployment strategy 2. Grid deployment. Network Simulator2 (NS2) delivers comparatively simulation results intended for the calculation of reliability and security.

***Index Terms*: AODV, DSDV, AMI Security, Routing**

I. INTRODUCTION

Smart meter is a vigorous fragment of the AMI provides bidirectional communication. Meter data management system is a heart of the system. Also communication infrastructure is an important part of the AMI. The stability and transmission rapidity of the communication infrastructure can be increased by using Power Line Communication. It is the low cost communication solution. It transfers the data in the form of high frequency signal. Instead of data transmission power transmission is done by the PLC. [1]. Enactment of the AMI grounded through different categories of networks (HAN, WAN) and control infrastructure. Metering provides different functions 1.Remotely we can check prizing 2.Reduces manual work. The main components of the AMI architecture are SM, wireless or wired communication technology, MDMS, data collector and system controller. The worldwide interoperability for microwave access (WiMAX) is unique wireless technologies for AMI. WiMax having very best features one of them it is suitable for long distances [2].Virtual private Networks (VPN) is the best option for secure connection in communication system of AMI. But the drawback is, it does not protect from the attack it just protect the tunnel [3]. In Demand Response Management(DRM), clients can modification their electricity consumption pattern through electricity tariff variations[4].For the security requirement of AMI confidentiality, integrity, key management, authentication needed[5].The performance of smart meter based on number of issues 1.energy 2.communication 3.data 4.real time alarms 5.costs and maintenance.

This paper basically concentrates on wireless communication security for AMI. For this number of things should be considered1. Communication infrastructure 2.Different protocols/Algorithms for wireless communication security3.Reliability of communication infrastructure 4.data security [6].This research focuses on only security parameter of the AMI communication. The number of researchers are doing work on the same parameter still there is a big issue. In power grid generation, delivery and consumption must happens at matching time that's why here communication, control and sensing infrastructure should be strong[7].And this is a challenge for the researchers. Data Acquisition system (DAS) can use in SG to acquire directly data in terms of current and voltage by reducing device required at the sensing point [8].The legacy of smart meter infrastructure essentials to be enhanced significantly, in terms of the following four significant facets 1.Inflexible for expansion 2.Inefficient 3.Unreliable 4.High cost [9].Accordingly the type of the network the wireless communication technologies will be use. Choosing of wireless technology is a big task for the AMI [10].Figure 1 gives brief idea about proposed AMI architecture for wireless communication security for AMI.

AMI and MDMS are fundamental of SG. AMI gathers and conveys smart meter data among devices and MDMS facilitates data gathering, storage and management. AMI architecture consists HAN, WSN, DC and MDMS. The attacker always think to do attack on MDMS and WSN. By doing attack on this part the AMI destroys the performance and all the system will troubled.

Manuscript published on 30 August 2019.
***Correspondence Author(s)**
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

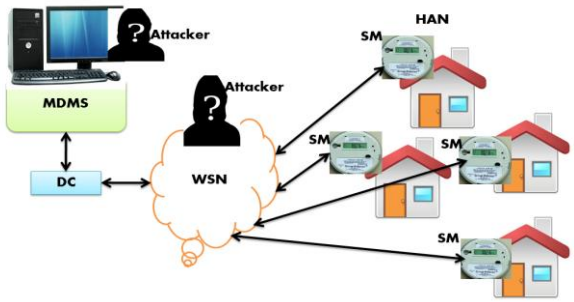


Fig. 1: AMI architecture (DC-Data Collector, WSN-Wireless Sensor Network)

A. MDMS

It manages all the important data. It gathers data from data collector. It accomplishes very significant role in SG.Figure2 provides the importance of MDMS for AMI. MDMS communicates with communication system, utility system, and AMI management system and data collector. It communicates bidirectional. Numerous diverse types of attacks occurs on MDMS. And due to this the system collapse. It degrade the AMI's performance. This paper tries to provide security for MDMS.

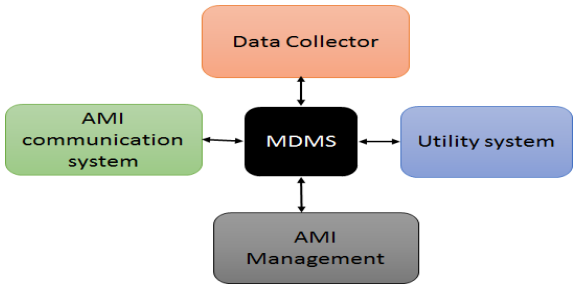


Fig. 2: MDMS

B. Communication infrastructure

Communication among AMI devices and the MDMS might be negotiated if the communication is not encrypted end-to-end. Authentication and authorization among devices must be encrypted to keep against rascal or damaged devices. Communication infrastructure basically depends on wireless communication technologies. From the table 1 it is clear that WiMAX, WSN, IOT, OFL and GPS are the preeminent choice for wireless communication

C. Wireless communication technology

Communication infrastructure plays vital role in the AMI. The performance of the communication infrastructure of the AMI depends upon different parameters basically type of communication technology, type of network, type of routing protocols and algorithms, Satisfaction of parameters of QOS. Basically in the AMI MDMS is important part. The attackers always try to stole the information or manipulate the information. The different parameters are considered for development of AMI mentioned in table1.

The number of researchers has worked on security of AMI by considering different architectural part. Still there is an immense problem of security parameter. Table 1 gives the information like AMI consists HAN, NAN, WAN, communication infrastructure, MDMS, distribution substation etc. Attacker creates the problem on each part of the AMI architecture. This paper focuses on security for wireless communication infrastructure for the AMI. This paper try to find different types of attack occurring on wireless communication preparation and also try to provide solution for the same by using efficient algorithm like AODSD2V2 by using NS2 simulation software and wireless sensor network. The performance calculation of AMI can be premeditated by seeing of privacy. Wireless message grids are more deserted to cyber-attacks. The many researchers proposing many security protocols still problem arises.IEEE802.11s and Zigbee are the wireless open source mesh networking standards. These try to provide security and privacy by providing Elliptic Curve Digital Signature Algorithm, Constrained Application Protocol used [27].Choosing an appropriate communication network is too much difficult because it based on number of parameters[28].For integration of building infrastructure and communication infrastructure interoperability essential[29].

II. DIFFERENT KINDS OF ATTACK ON AMI AND THEIR SOLUTION

AMI have a big infrastructure for automation and communication infrastructure. The different kinds of attack occurs on each part of the AMI. This paper focuses on communication infrastructure of the AMI. This research reviews on different kinds of attack occurred on communication infrastructure and their solution. Cyber security for the AMI is the key element for the AMI development**.** Table 2 gives the information for the same.

III. ATTACK ON COMMUNICATION INFRASTRUCTURE AND THEIR SOLUTION

NAN is a part of communication infrastructure of the AMI. Constantly attacker try to do attack on network area of the AMI. Electricity theft directly take power lines, it is a big issue. The many researchers had done work on it. Still problem not solved. For this problem researchers are doing work on it. The researcher has proposed two algorithms for the same 1.MCGI2. G-BCGI. Here users ID's are encoded in binary notation. Both are most proficient algorithms [30].In AMI two kinds of losses occurs 1.Technical losses 2.Non-technical losses[31].wireless physical layer security provides with the help of received signal strength(RSS) based protocol. Monte Carlo simulator is recycled for the analysis of the performance [32].The classification of threats accordingly their sources in SG 1.Technical source of threats 2.Non-technical source of threats. Security is a vast dispute. It's not solved easily while providing security we have to think different possibilities accordingly their classification. Different framework supports to isolate different causes of threats [30]. Without increasing the period of key circulation and the communication overhead the researcher try to provide security for unicast, multicast and broadcast communications by considering security level confidentiality, integrity, availability and accountability.

Retrieval Number: I8178078919/19©BEIESP
DOI: 10.35940/ijitee.I8178.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Table 1: Development of AMI in terms of different parameters *(Part 1)*

Ref. No.	Type of network mentioned	Type of wireless communication technology	Considered attacks	Methodology	Simulation platform/ Software	Considered parameters
11.	Wireless Area network	M2M and IOT	Cyber attacks	IOT implementation of sensor network	Building controls virtual bed (BCVTB) software	granularity, accuracy, cost, availability, ease of deployment
12.	Distribution Networks	Wifi,zigbee,PLC,6LowPan		Cloud solution ,real-time distributed state estimation algorithm	cloud-based software platform, (aka Flex meter)	scalability, interoperability and flexibility
13.	suburban neighborhood topology,Adhoc (meshmode)		Flooding attack, spoofing, DOS	Flooding awareness AODV(FLOW-AODV)	NS3	Packet delivery ratio and average delay
14.		M2M,4G worldwide Interoperability for Microwave Access	Cyber-attacks,DOS, large scale, physical attacks	Public Key Infrastructure, Dynamic Stochastic Optimal Power Flow computational algorithm		Security challenge framework, Confidentiality, authentication and privacy, reliability and efficiency, resiliency
15.	LMN, HAN, WAN	smart meter gateway(SMGW)		IP based protocols, automation protocol, Cryptographic protocol, serial protocol	Transparency software, third party software	authentication and authorization
16.	NAN,WAN	RS485, Power Line Carrier, Zig Bee and GPRS/3G, Ethernet	Energy theft attacks physical attacks, contami-nation attacks	linear programming (LP)	Matlab R2014b	Loss factor, error term, noise
17.	Neural networks, WSN			Data compression methods-Lossy compression, WT, SAX, PCA, SVD, LZ algorithms, Huffman coding		Data mining efficiency, overhead and transmission pressure reduced form, smart meter big data compression. loss ratio
18.	HAN,NAN,WAN ,IP based digital network, (SANETs) Sensor / actuator networks	IOT	Cyber-attacks, physical attacks	contingency management,IoT paradigm, Power point tracking algorithm,Welch-based application algorithm, machinel learning algorithms, Controlalgorithms,Communication protocol and internet protocol	Workplace software, progressive software	interoperability and connectivity, cyber security
19.	BAN,NAN,HAN	Microcontroller ARM	well-known attacks	ECC	*ProVerif* tool	fast and secure communications, Computational and communication Costs.
20.	Privacy preserving nodes		Filtering and true value attacks	data perturbation, Holt-Winters and STL methods, encryption and decryption methods,combination ofencryption and perturbation techniques, Shamir'sSecret Sharing algorithm		Privacy, security, integrity

Table 1: Development of AMI in terms of different parameters (*Table 1 continued…..)*

Ref. No.	Type of network mentioned	Type of wireless communication technology	Considered attacks	Methodology	Simulation platform/ Software	Considered parameters
21.	Low Power Wide Area Networks, traditional Wireless Sensors Networks, Peer-to Peer, Convolutional Neural Networks, fuzzy neural networks	IOT	Device trigger attacks, cyber-attacks, security attacks, eavesdropping and injection attack, replay attack, spoofing, manipulation attack etc.	AODV, elliptic curve digital signature algorithm, FHC algorithms, digest algorithms		security/privacy
22.	Cellular system, HAN	GPS	Interception/injection/blocking	Zig Bee radio Protocol, communication protocol stack		Security(confidentiality, integrity and availability)
.23.				P2Q scheme, CP-ABE scheme		Privacy preservation, confidentiality
24.	HAN,WAN	Lot of mentioned comparatively	DOS	secure smart- metering protocol (SSMP),voice over internet protocol (VoIP),		security
25.	Cyber-Physical Systems (CPS)	SCADA	Cyber attacks	IP protocol, communication protocol etc.		Cyber security, information security
26.	Distribution network		Cyber attacks	IP protocol, communication protocol etc.		Cyber security

Table 2: Diverse types of attacks and their solution for the AMI

Ref. No.	Type of Attack considered	Proposed algorithm/protocol/methodology	Simulation platform
11.	Cyber-attack, deliberate attacks	Control algorithms	BACnet interface (building controls virtual bed (BCVTB) to couple EnergyPlus1with control systems.)
13.	Flooding attack, DOS, Route Request (RREQ) flooding, puppet attack	FLOW-AODV based algorithm	NS3
16.	cyber-attacks, network-borne attacks, contamination attacks/non-malicious factors, energy theft attacks, NTLs attack, zero-day attack, physical attacks, data attacks, diverse and sophisticated attack,	Communication protocols, adapts Internet protocols, ADF scheme, Enhanced ADF scheme, linear programming	Matlab R2014b
18.	Physical attack, Resist attack, cyber-attack, individual consumer's data attack	power point tracking algorithm, control algorithm, Welch-based application algorithm, machine learning algorithms,	workplace software, big data analytics and progressive software
19.	well-known attacks, false data injection attack, modification attacks	symmetric encryption/decryption algorithm,	
20.	Value attack	Shamir's Secret Sharing algorithm, multi-key algorithm, Task-Assign Algorithm, Seasonal Trend Decomposition using Loess (STL)	
22.	Bricking attack, cyber-attack, possible attack, true attack, interception, modification, fabrication, interruption, injection blocking	Communication channel protocol,zigbee radio protocol, ISM protocol	
24.	Physical layer attack, DOS, cyber attack	PKI technology, encryption algorithm, communication algorithm, sophisticated processing algorithm	
25.	Dos, cyber, reflect attack	TCP/IP protocol, communication protocol	
26.	Cyber security	IEC TC 57,IEC 62351	

IV. DIFFERENT SIMULATION PLATFORM FOR THE CALCULATION OF THE PERFORMANCE OF WIRELESS COMMUNICATION SECURITY

In this paper we focus on communication network simulator. Different performance metrics of AMI communication network calculated accordingly data rate, reliability and security. In SG environment, simulators permit to learning difficult relations among these interconnected systems and the checking and control elements on upper of them. The NS2, NS3, MATLAB Modeler are the commonly used simulation tools in communication network of the AMI [40].

Table 3: Different types of simulators for evaluation of WSN [40][41]

Different types of simulators for different level	Simulators
Topology control simulator (The simulator comes with a tool for topology generation based on different distributions and a visualization interface)	Atarraya.(open source simulators)
NS-2 based simulators(mainly used in the studies of TCP, routing and multicast protocols)	Mannasim, NRL Sensorsim, RTNS etc.(open source simulators)
OMNeT++ constructed emulators(widely used in other research areas, such as queuing systems or hardware emulation)	open source
Ptolemy II based simulators(Software components, called actors, execute simultaneously, exchanging messages through interconnected ports and thus form hierarchical structures of models)	Viptos, Visual Sense, etc.(open source simulators)

To meet security requirements and confirm secure transportations in AMI, cryptographic counter processes obligation to be arranged [33].Two acute issues when emerging the technical requirements of the SG communication infrastructure are QoS and security. WiMax technology can be used for the reliable elongated distance communication of rustic areas. WiMax supports 5 levels of QoS to agree unlike packets to be given unlike service [34].NTP is a synchronization protocol which is best for time synchronization by providing synchronization jitter [35].Data delivery packet reassembly problem occurs. Many times attacker try to attack on transmission of data that time data should be resend. For that new secure MPC-based protocol available. It also try to maintain security aspect [36].To provide interoperability for communication infrastructure is a challenge in AMI infrastructure[37].For strong communication networking researchers have to do work hard like communication protocol, QOS, time synchronization communication routing protocol, energy web, HAN,NAN, WAN[38]. A Decentralized Efficient Privacy-Preserving and Selective Aggregation Scheme (DEP2SA) more powerful try to provide security for AMI. Homomorphic encryption techniques are used [39].

3.1Network Simulator (NS2/NS3)

It is contented with C++ language and OTcl [40].NS2 is open source software.NS3 is still in growth process.it is same like NS2 but some advance features are supplementary [41].

3.2 OMNeT++:

It supports both wired and wireless communication. It supports much protocol which is used for communication purpose [40].

3.3 Network Simulator Software (NeSSi):

Distributed Artificial Intelligence Laboratory (DAIL) supported to NeSSi. It supports to modeling of attack, attack detection and security metrics. It is one of the best simulations for calculation of security metrics [40].

3.4 OPNET Modeler:

This simulation platform is contented with C and C++ language. Path loss, mobility and latency can calculate [40].Table 3 offering for researchers to get the information regarding WSN simulators having different options [41]

V. RESULT

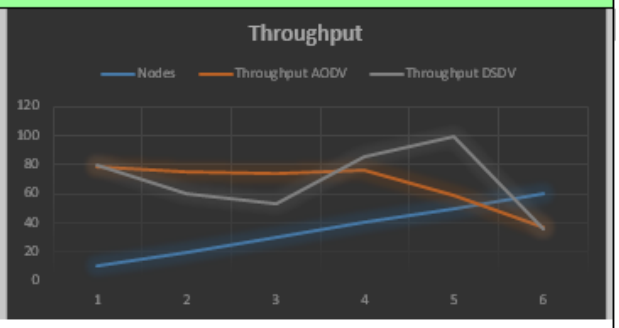
WSN provides design and evaluation of attack model for proactive and reactive protocols technology. Also for security requirement proper routing performs a vital role. Table 4.appearances the actual design considering AODSD2V2 protocol [42]. By mingling different technologies defiantly we accomplish good concert of security. Table 4.provides brief information of designing parameters. With the aid of this table 4. By coalescing AODV and DSDV that is AODSD2V2 we got different results. We completed simulation by using NS2.AODSD2V2 tries to provide best path to transfer the different packets to the nodes by checking the situation of nodes. If the node is malicious it will inform. This research combine features of AODV and DSDV and provides efficient path to transfer the packets in WSN by considering delay, energy consumption, PDR, throughput and overhead. AODV provides unicast and multicast routing. DSDV have to update table accordingly the situation. The performance of DSDV totally dependent on the routing table. It does not deliver multipath routing [43]. Distributed Bellman-Ford algorithm is used for the employment of DSDV protocol [44].WSN supports multipath routing using dynamic topology [45].WSN performance is based on selection of sensor nodes. Nodes should be strong. It should not be malicious consequently secure routing protocols should be needed.

WSN is auspicious machinery for SG. It expands the performance of SG providing secure sensor nodes. AMI communication infrastructure should be strong and secure. WSN tries to provide good communication infrastructure for AMI [46]. Table 5.provides simulation results of attack model using WSN. For simulation NS2 is used. Different types of Dos attacks are considered.AODS2DV improves security considering: **Delay, Throughput, Energy consumption, Packet Delivery Ratio, overhead.**

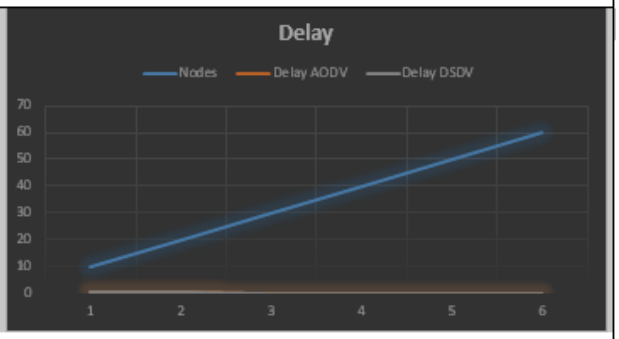
Table 5: Simulation results

Security improvement in terms with Throughput, Delay, PDR, energy consumption and overhead For AMI.	Simulation results using NS2

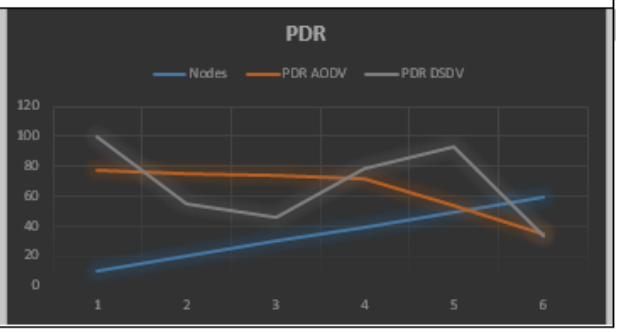
	Throughput	
Nodes	AODV	DSDV
10	78.58	79.4
20	75.32	59.62
30	74.18	53.4
40	76.21	85.3
50	59.07	99.43
60	37.44	35.71



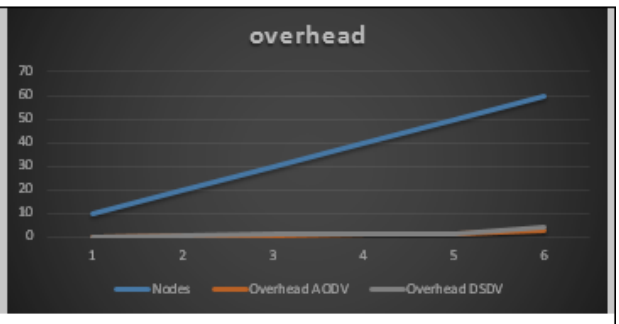
	Delay	
Nodes	AODV	DSDV
10	0.07408	0.2667
20	0.08628	0.2142
30	0.01885	0.018
40	0.009493	0.01137
50	0.006316	0.0093
60	0.00178	0.001086



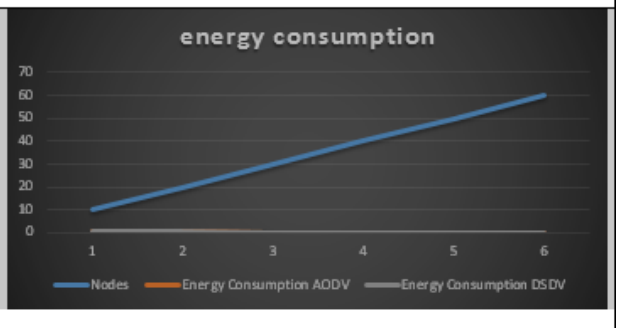
	PDR	
Nodes	AODV	DSDV
10	77.79	100
20	74.96	54.85
30	74.62	46.353
40	71.51	78.26
50	54.05	92.69
60	34.45	33.33



	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



	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



Retrieval Number: I8178078919/19©BEIESP
DOI: 10.35940/ijitee.I8178.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Table 4: Design and evaluation of attack model considering AODV and DSDV protocols.

Design and Evaluation of Attack Model for Proactive and Reactive Protocols	
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 and DSDV (Proactive and Reactive) Simulation Time: 100 seconds Performance Metrics: **Throughput, Delay, Packet Delivery ratio, Overhead, Energy consumption** (all parameters calculated considering 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, Delay, Packet delivery ratio, Overhead Energy consumption** (all parameters calculated considering number of nodes.)

AODSD2V2 calculates throughput, it should be high and AODV provides it high. AODSD2V2 calculates delay, it should be less and AODV provides it less. AODSD2V2 calculates PDR, it should be high and AODV and DSDV provide it high. AODSD2V2 calculates overhead, it should be low and AODV and DSDV provide it near about same. AODSD2V2 calculates energy consumption, it should be low and AODV and DSDV provide it near about same. From this research it is clear that AODV and DSDV is not enough for secure AMI communication. By combining AODV and DSDV we can increase secure communication still having problem of secure communication.

VI. CONCLUSION

Ultimately, computing routing performance of WSN for AMI we can provide security and reliability. For the worthy enactment of the network routing to be authentic. Using NS2 calculated delay, PDR, throughput, energy consumption and overhead. Consequently the simulation result of AODV and DSDV in accordance with density we have intended security. By combining AODV and DSDV we can increase little bit security parameter still having big issue. Since AODV and DSDV are not having strong provisions to tackle different kinds of attacks.

VII. FUTURE SCOPE

Eventually, the numerous researchers are working on security dispute of the AMI still having AMI and electricity sector deficient to provide security. From the paper it is clear that AODSD2V2 is not efficient security protocols. It provides slight security. Consequently electricity sector appearances lot of problems. And it degrades the performance. The many researchers have a lot of scope to do research work by considering different types of networks, Different secure algorithms and different secure protocols. Also considering different kinds of attacks.

REFERENCES

1. Jun-Ho Huh, Sugarbayar Otgonchimeg, Kyungryong Seo1. Advanced metering infrastructure design and test bed experiment using intelligent agents: focusing on the PLC network base technology for Smart Grid system; May 2016, Volume 72, Issue 5, pp 1862–1877.
2. Yasin Kabalci. A survey on smart metering and smart grid communication; Volume 57, May 2016, pp 302-318
3. 3.Charalambos Konstantinou, Michail Maniatakos, Fareena Saqib, Shiyan Hu, Jim Plusquellic and Yier Jin. Cyber-Physical Systems: A Security Perspective; Date of current version January 20, 2016.Digital Object Identifier 10.1109/ACCESS.2016.2516158, 2015 20th IEEE European Test Symposium (ETS).
4. IEEE ACCESS SPECIAL SECTION EDITORIAL SMART GRIDS: A HUB OF INTERDISCIPLINARY RESEARCH;,10.1109/ACCESS.2016.2516158:EDITORIAL
5. Fisnik Dalipi, Sule Yildirim Yayilgan. Security and Privacy Considerations for IoT Application on Smart Grids: Survey and Research Challenges; 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), DOI: 10.1109/W-FiCloud.2016.28.
6. Jaime Lloret, Jesus Tomas, Alejandro Canovas, and Lorena Parra. An Integrated IoT Architecture for Smart Metering; IEEE Communications Magazine, Volume: 54, Issue: 12, December 2016.
7. Stefano Galli, Thierry Lys. Next Generation Narrowband (Under 500 kHz) Power Line Communications (PLC) Standards; Volume: 12, Issue: 3, Mar. 2015.
8. Damminda Alahakoon, Member, IEEE, and Xinghuo Yu, Fellow, IEEE. Smart Electricity Meter Data Intelligence for Future Energy Systems: A Survey; Volume: 12, Issue: 1, Feb. 2016.
9. Yu Yan, Wencong Su. A Fog Computing Solution for Advanced Metering Infrastructure;2016 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)
10. Anzar Mahmood, NadeemJavaid, SohailRazzaq. A review of wireless communications for smart grid; Volume 41, January 2015, pp248-260.
11. Muhammad Waseem Ahmad, Monjur Mourshed, David Mundow, Mario Sisinni, Yacine Rezguia. Building energy metering and environmental monitoring – A state-of-the-art review and directions for future research; Volume 120, 15 May 2016, pp. 85-102.
12. Marco Pau, Edoardo Patti, Luca Barbierato, Abouzar Estebsari,Enrico Pons, Ferdinanda Ponci, Antonello Monti. A cloud-based smart metering infrastructure for distribution grid services and automation; Volume 15, September 2018, pp. 14-25.
13. Md Raqibull Hasan, Yanxiao Zhao, Yu Luo, Guodong Wang, Robb M Winter. An Effective AODV-based Flooding Detection and Prevention for Smart Meter Network; Volume129, 2018, pp. 454-460.
14. Abdulrahaman Okino Otuoze, Mohd Wazir Mustafa, Raja Masood Larik. Smart grids security challenges: Classification by sources of threats; February2018.
15. Jurgen Meister, Norman Ihle, Sebastian Lehnhoff, Mathias Uslar.Smart grid digitalization in Germany by standardized advanced metering infrastructure and green button; 2018, pp. 347-371.
16. Sook-Chin Yip, Wooi-Nee Tan, ChiaKwang Tan, Ming-Tao Gan, KokSheik Wong. An anomaly detection framework for identifying energy theft and defective meters in smart grids; Volume101, October 2018, pp.189-203.
17. Lulu Wen, Kaile Zhou, Shanlin Yang, Lanlan Li. Compression of smart meter big data: A survey; Volume91, August 2018, pp.59-69.

18. S. Sofana Reka, Tomislav Dragicevic. Future effectual role of energy delivery: A comprehensive review of Internet of Things and smart grid; Volume91, August 2018, pp. 90-108.
19. 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; Volume 40, June 2018, pp. 9-19.
20. Ulas Baran BALOGLU, Yakup DEMİR. Lightweight Privacy-Preserving Data Aggregation Scheme for Smart Grid Metering Infrastructure Protection; Volume22, September 2018, pp. 16-24
21. Hadi Habibzadeh, Tolga Soyata, Burak Kantarci, Azzedine Boukerche, Cem Kaptan. A Survey of the Sensing, Communication, and Security Planes in Smart City System Design; Volume 144, 24 October 2018, pp.163-200.
22. Aaron Hansen, Jason Staggs, Sujeet Shenoi.Security analysis of an advanced metering infrastructure; Volume 18, September 2017, pp.3-19.
23. Rong iang Rongxing LuKim-Kwang Raymond Choo.Security analysis of an advanced metering infrastructure; Volume 18, September 2017, Pages 3-19.Achieving high performance and privacy-preserving query over encrypted multidimensional big metering data; Volume 78, Part 1, January 2018, pp. 392-401.
24. Yasin Kabalci.A survey on smart metering and smart grid communication; Volume 57, May 2016, PP302-318.
25. Rafał Leszczyna. A Review of Standards with Cyber security Requirements for Smart Grid; Volume 77, August 2018, pp. 262-276.
26. Rafa l Leszczyna.Standards on Cyber Security Assessment of Smart Grid; Volume 22, September 2018, pp.70-89.
27. Samet Tonyali, Ruben Munoz, Kemal Akkaya, Utku Ozgur. A Realistic Performance Evaluation of Privacy-Preserving Protocols for Smart Grid AMI Networks; Volume 119, 1 October 2018, pp 24-41.
28. Haider TarishHaider, OngHangSee, WilfriedElmenreich. A review of residential demand response of smart grid; Volume 59, June 2016, pp 166-178.
29. D. Kolokotsa. The role of Smart Grids in the Building Sector; Volume 116, 15 March 2016, pp 703-708
30. Abdulrahaman Okino Otuozea, Mohd Wazir Mustafaa, Raja Masood Larik. Review Smart grids security challenges: Classification by sources of threats; 7 February 2018.
31. Esther Villar-Rodriguez, Javier Del Ser, Izaskun Oregi, Miren Nekane Bilbao, Sergio Gil-Lopez. Detection of non-technical losses in smart meter data based on load curve profiling and time series analysis; Volume 137, 15 October 2017, pp 118-128.
32. 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; Volume 78, September 2018, pp 454-476.
33. Mourad Benmalek, Yacine Challal, Abdelouahid Derhab, Abdelmadjid Bouabdallah. VerSAMI: Versatile and Scalable key management for Smart Grid AMI systems; Volume 132, 26 February 2018,pp 161-179
34. Stefano Rinaldi, Davide Della Giustina, Paolo Ferrari, Alessandra Flammini, Emiliano Sisinni. Time Synchronization over Heterogeneous Network for Smart Grid Application: Design and Characterization of a Real Case;
35. Stefano Rinaldi, Davide Della Giustina, Paolo Ferrari, Alessandra Flammini, Emiliano Sisinni. Time Synchronization over Heterogeneous Network for Smart Grid Application: Design and Characterization of a Real Case; Volume 50, 1 November 2016, pp 41-57.
36. Samet Tonyali, Kemal Akkayaa, Nico Saputro, A. Selcuk Uluagac, Mehrdad Nojoumian.Privacy-preserving protocols for secure and reliable data aggregation In IoT-enabled Smart Metering systems; Volume 78, Part 2, January 2018, pp 547-557.
37. Michael Emmanuel, Ramesh Rayudu. Communication Technologies for Smart Grid Applications: A Survey; Volume 74, October 2016, pp 133-148.
38. Mehmet H. Cintuglu, Osama A. Mohammed, Kemal Akkayaand, A. Selcuk Uluagac. A Survey on Smart Grid Cyber-Physical System Test beds; Volume: 19, Issue: 1 , First quarter 2017.
39. MUSTAFA A. MUSTAFA, NING ZHANG, GEORGIOS KALOGRIDIS, AND ZHONG FAN. DEP2SA: A Decentralized Efficient Privacy-Preserving and Selective Aggregation Scheme in Advanced Metering Infrastructure; 07 December 2015.
40. Kevin Mets, Juan Aparicio Ojea, Chris Develder. Combining Power and Communication Network Simulation for Cost-Effective Smart Grid Analysis;
41. Patel Rajankumar, Patel Nimisha, Dr.Pariza Kamboj. A Comparative Study and Simulation of AODV MANET Routing Protocol in NS2 & NS3;
42. Kirti A. Yadav and P. Vijayakumar, "VANET and its Security Aspects: A Review" Indian Journal of Science and Technology, Vol 9(44), DOI: 10.17485/ijst/2016/v9i44/97105 November 2016.
43. Noor H. BHANGWAR, Imtiaz A. HALEPOTO, Intesab H. SADHAYO, Suhail KHOKHAR, Asif A. LAGHARI, " On Routing Protocols for High Performance",Studies in Informatics and Control, 26(4) 441-448, December 2017.
44. A. A. Chavan, Prof. D. S. Kurule, Prof. P. U. Dere, "Performance Analysis of AODV and DSDV Routing Protocol in MANET and Modifications in AODV against Black Hole Attack" 7th International Conference on Communication, Computing and Virtualization 2016, science direct.45. Anand Nayyar, Rajeshwar Singh , "Simulation and Performance Comparison of Ant Colony Optimization (ACO) Routing Protocol with AODV, DSDV, DSR Routing Protocols of Wireless Sensor Networks using NS-2 Simulator", American Journal of Intelligent Systems 2017, 7(1): 19-30 DOI: 10.5923/j.ajis.20170701.02
45. Sana Rekik, Nouha Baccour, Mohamed Jmaiel, Khalil Drira, "Wireless Sensor Network Based Smart Grid Communications: Challenges, Protocol Optimizations, and Validation Platforms" _Springer Science+Business Media New York 2017.
46. R. J. Vidmar. (1992, August). On the use of atmospheric plasmas as electromagnetic reflectors. *IEEE Trans. Plasma Sci.* [Online]. *21(3).* pp. 876—880. Available: http://www.halcyon.com/pub/journals/21ps03 -vidmar

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