SRAMI: Secure and Reliable Advanced Metering Infrastructure Protocol for Smart Grid

Priyanka Halle (priyankahalle500@gmail.com)
Vel Tech Rangarajan Dr Sagunthala R&D Institute of Science and Technology
Shiyamala S.
Vel Tech Rangarajan Dr Sagunthala R&D Institute of Science and Technology

Research Article

Keywords: Advanced metering infrastructure, cryptography, elliptic curve cryptography, reliability, smart grid, security, wireless sensor network

Posted Date: September 21st, 2021

DOI: https://doi.org/10.21203/rs.3.rs-791353/v1

SRAMI: Secure and Reliable Advanced Metering Infrastructure Protocol for Smart Grid

Priyanka D. Halle*
PHD scholar, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamil Nadu, India.
hallepriyanka2011@gmail.com
Dr. Shiyamala S.
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamil Nadu, India
drshiyamala@veltech.edu.in

Abstract: The emergence of Advanced Metering Infrastructure (AMI) into the Smart Grid applications receiving significant attention by researchers of the Internet of Things (IoT) assisted smart city projects. Communication networks (WiFi/WLAN) is one of the key building blocks of AMI for information exchange. The wireless communication networks are vulnerable to various security threats that lead to problems in designing the AMI system in smart city projects. The main requirements of cyber-physical systems like AMI include confidentiality, integrity, availability, and privacy. To satisfy the requirements of cyber-physical systems, we focused on the wireless communication protocol that addresses data transmission reliability and data security with minimum power consumption and overhead. The Secure and Reliable AMI (SRAMI) protocol using the unique trust-based mechanism for reliability and lightweight cryptography mechanism for the security proposed for Wireless Sensor Network (WSN)-assisted AMI. The trust-based algorithm introduces to establish a reliable data transmission technique among two communicating entities of AMI. In this regard, next-hop selected according to trust-evaluation using parameters energy consumption, geographical distance, and bandwidth availability parameters. Furthermore, the lightweight Elliptic Curve Cryptography (ECC)-based hybrid technique introduces to satisfy the data integrity and privacy requirements in the AMI network. The performance of SRAMI evaluated using throughput, Packet Delivery Ratio (PDR), average energy consumption, delay, and communication overhead compared to state-of-art methods. The throughput and PDR improved by 5 % and 3.14 % compared to existing methods. The energy consumption, delay, and overhead reduced by 7.36 %, 12.16 %, and 17.66 % compared to existing techniques.

***Keywords*:** Advanced metering infrastructure, cryptography, elliptic curve cryptography, reliability, smart grid, security, wireless sensor network

1 Introduction

AMI (Advanced Metering Infrastructure) is the common terminology to explain the entire infrastructure of Smart Meter to two way-communication interfaces to manage center devices and all the pertinence that facilitate the collection and transfer of power utilization data in imminent real-time [Fadlullah et al. 2018]. AMI delivers two-way communications with consumers desirable and is the resolution of the smart grid. The purposes of AMI can be network difficulty credentials, smart meter reading for error-free data, partial load reduction, energy examination, and load profiling in place of load molting [Huh et al. 2016]. AMI consists of different hardware and software segments, all of which represent a function in regulating power consumption and communicating data about power, gas, and water usage to service organizations and consumers. The technological elements of AMI incorporate:

- ***Smart Meters:*** These AMI elements having the capacity to gather data about power, water, and gas usage at periodic intervals and communicating the data over established communication networks to the utility, and getting data like pricing signals from the utility and sending it to the customer. The smart meters can represent as sensor devices.
- ***Communication Network:*** The data transmission among smart meters and the utilities performed using two-way communication technique. The commonly used communication methods are Power Line Communications (PLC), Broadband over Power Line (BPL), Fixed Radio Frequency (FRD), Fiber Optic Communication (FOC), or public networks (e.g., landline, cellular, paging).
- ***Meter Data Acquisition System:*** As the name indicates, this component deals with data acquisition from the meters through the communication network and transmits it to the Meter Data Management System (MDMS) using communication networks.
- ***Meter Data Management System (MDMS):*** This is the host component that collects, stores, and examines the metering data.

The AMI benefits several ways in the Internet of Things (IoT) enabled smart city applications such as operational benefits, financial benefits, and customer benefits [Muhanji et al. 2019]. For operational benefits, AMI helps the whole grid by advancing the efficiency of meter reading, power theft detection, and reply to power interruptions while reducing the demand for an on-site meter reading. For financial benefits, AMI produces economic profits for utility, water, and gas organizations by decreasing material and support prices, facilitating the faster rehabilitation of electrical assistance through blackouts, and streamlining the billing method. For customer benefits, AMI avails electric consumers by identifying meter malfunctions early, providing quick assistance recovery, and enhancing the efficiency and versatility of billing. It supports time-based rate choices that can assist consumers in managing their power consumption and save money [Al-Turjman et al. 2019]. However, AMI deployment suffers from various challenges such as security against cyber threats, reliability, energy theft, energy costs, integration, etc. AMI is a kind of cyber-physical system in IoT applications and suffers from different security

threats. Hence, protecting the AMI data communications between smart meters and AMI hosts from various cyber threats is a research problem. From the perspective of the smart city project, AMI becomes a crucial part of the IoT-assisted systems. As discussed earlier, the smart meters periodically sense the meter data and transmit it to the AMI host via insure wireless communications. Thus, to protect such insecure communications in AMI from cyber threats, two mechanisms need to be done at the network layer like reliable route discovery and secure data transmission. These two mechanisms bring security benefits using AMI to the smart grid systems and consumers.

Smart Grid saves millions of dollars in the electricity sector by providing smart and secure wireless communication infrastructure to AMI. The communication from smart meters (acts sensor nodes) to the AMI hosts (acts base station node) represents the Wireless Sensor Network (WSN)-assisted IoT system for AMI [Barsana et al. 2021]. The wireless networks like Mobile Ad hoc Network (MANET) and WSN are self-configured enabling technologies and enhancing the performance of Quality of Services (QoS) for these enabling technologies is a challenging task [Mahajan et al 2018]. WSN and MANET suffer from performance degradation due to diverse threats, corresponding forging, Replay, Colluding, Denial of Service (DoS), and Malicious attacks [Singh et al. 2018]. This research focuses on designing routing protocol to address the challenges of reliability and data security in presence of cyber threats via the calculation of parameters PDR, output quantity (throughput), communication delay, communication overhead, and energy consumption. Several routing protocols introduced categories-wise on-demand, table-driven, hybrid, etc., but such protocols failed to protect network communications from security threats [Lekshmi et al. 2020]. Proactive Ad-hoc On-demand Distance Vector (AODV) and reactive Destination-Sequenced Distance-Vector Routing (DSDV) are non-secure routing protocols with no provisions to tackle malicious attacks. The AODV and DSDV investigators were annoyed to provide routing security for MANET and WSN considering routing calculation parameters, and their effect on security was despicable for wireless communication [NC et al. 2018]. Subsequently the failures of the non-secure protocols, researchers are tried cryptography-based protocols like Authenticated Anonymous Secure Routing (AASR) [Liu et al. 2014] and trust-based Trusted and Energy-efficient Routing Protocol (TERP) [Shen et al. 2017], but such approaches failed to satisfy all the security requirements.

To gain the security benefits in AMI, we proposed the Secure and Reliable AMI (SRAMI) routing protocol using the lightweight ECC-based cryptography and trust-based approach for reliable route discovery. The goal of the SRAMI protocol is to satisfy all the security requirements of AMI communications that include confidentiality, integrity, availability, and privacy. Figure 1 demonstrates the mechanism of SRAMI protocol for smart grid AMI application. The trust-model introduces reliable next-hop selection and ECC-based lightweight cryptography for secure data transmission. The performance of SRAMI is satisfied by the five QoS parameters PDR, throughput, communication delay, communication overhead, and average energy consumption of smart meters. Section 2 presents a brief study on the state-of-art methods. Section 3 presents the algorithms of the SRAMI protocol. Section 4 presents the simulation results and discussions. Section 5 presents the conclusion

and future recommendations.

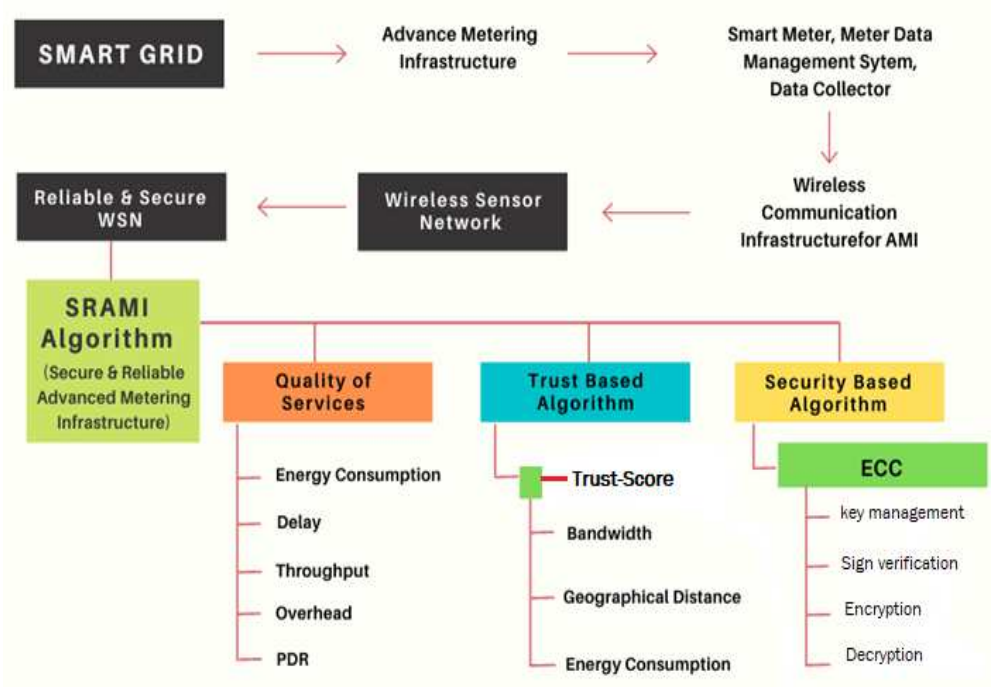

Figure 1. AMI Optimization via security benefits using trust and cryptography-based approaches

2 Related work

Since the past decade, several attempts introduced for the security of wireless networks such as WSNs, MANET, and IoT-enabled networks to protect against the various threats. The methods are broadly categorized into trust-based and cryptography-based for attack detection and mitigation during the wireless data transmissions. This section reviewed some recent trust-based and cryptography-based mechanisms for wireless communications. After that, research motivations and contributions have been disclosed.

A. Wireless Security Methods

Conviction management is a big challenge in a different wireless communication network, even though researchers are attempting to give security issues are not finished [Kraounakis et al. 2015]. All the aspects of the SRAMI algorithm are demonstrated. Researchers, who had worked on security issues for different types of networks, still face difficulties.

Ou et al. (2009) introduced the first study on trust-based security for wireless networks. They presented a trust evaluation model using direct trust computation and

indirect trust computations. Das et al. (2012) proposed the "SecureTrust" protocol for Peer to Peer (P2P) network communications. They analyzed various parameters of trust and designed the model to compute the trust score. The load-balancing mechanism was designed using trust models as well. Liu et al. (2014) introduced a cryptography-based protocol to secure wireless communications in MANETs. They proposed Authenticated Anonymous Secure Routing (AASR) to protect against security threats. They proposed the key-encrypted onion routing mechanism with verification of route secrete messages. Tan et al. (2016) proposed a hybrid approach for network security using the trust management system and cryptography operations. They integrated the proposed model with the Optimized Link State Routing (OLSR) protocol. Pavithira et al. (2016) had tried to enhance the security by using a hash message authentication code by considering forging, replay, and colluding attacks for Vehicular Ad hoc Networks (VANETs). Shen et al. (2017) proposed a novel routing solution called TERP (Trustworthiness Evaluation-based Routing Protocol) to protect VANET communications from attackers. They computed the trustworthiness of each vehicle via cloud where the corresponding vehicle parameters were uploaded. The trustworthiness evaluation of nodes was used to select reliable forwarding nodes. Singh et al. (2017) integrated trust management and ECC-based mechanisms proposed for MANET. The trust was categorized into three various trust levels according to Schnorr's signature and ECC. Sultana et al. (2017) proposed secure data transmission in MANET using the ECC technique into the existing AOMDV (Ad hoc On-demand Multipath Distance Vector) protocol. Ramesh et al. (2019) proposed a lightweight trust-based decision-making approach for secure routing for both intra-cluster and inter-cluster communications for WSNs. Alshehri et al. (2019) proposed the fuzzy-based mechanism to detect the on-off attacks involved in bad service provisioning. They designed a secure data transmission algorithm to transmit data between intended nodes. Selvi et al. (2019) proposed an energy-efficient trust-based routing mechanism. They designed the trust evaluation model to detect the malicious nodes in WSN. The Spatio-temporal constraints were applied for best route selection. Mahantesh et al. (2020) designed a secured communication method to evaluate comprehensive trust scores for the target relay node and they applied a reputation score approach to select the legitimate forwarding node. For authentication, they used the progressive key generation approach. Yu et al. (2020) proposed ETM (Energy Trust Model) using node trust and remaining energy. They further designed TSDDR (Trust-based Secure Directed Diffusion Routing Protocol) using ETM for WSN. Kore et al. (2020) proposed a cross-layer trust model called IC-MADS (IoT enabled Cross-layer Man-in-Middle Attack Detection System). They designed IC-MADS in two phases clustering and attack detection. Poomagal et al. (2020) proposed secure data transmission among the vehicular nodes using ECC. They designed ECC for satellite communication and key agreement for secure message transmission. Ali et al. (2020) proposed data security mechanisms in WSN with minimum response time and computational efforts. They designed modified Diffie-Hellman for secure communications in WSN. AlMajed et al. (2020) proposed authenticated encryption based on plain text improved mapping phase into the elliptic curve to protect against various security threats. Chaitra et al. (2021) proposed SEEDT (Secure and Energy-Efficient Data Transmission) proto-

col. The clustering performed by multi-objective function and ECC used for secure data transmission in WSN.

Table 1. State-of-the-art of the wireless network with security solution

Reference	**Considered Wireless network**	**Proposed methodology /protocol /algorithm**	**Considered parameters**	**Considered Attack**
Ou et al. 2009	Not Applicable	Trust model based on TPM	Communication trust-based management, information security	Not Applicable
Das et al. 2012	P2P networks	Trust-based security and load balancing algorithm	Communication security	Malicious attacks
Liu et al. 2014	MANET	AASR	Communication security (throughput increases, PDR increases)	DoS
Tan et al. 2016	Ad hoc Network	OLSR protocol	Data plane security	Data plane attacks
Pavithira 2016	VANET	Hash message authentication code	Communication security and message authentication, efficiency (delay decreases, PDR increases)	forging, Replay, Colluding
Shen et al. 2017	VANET/self - configured network	TERP protocol	Communication security (QoS parameters)	Not Applicable
Singh et al. 2017	MANET	Trust management with ECC	MANET (QOS parameters)	black hole, flooding and selective packet dropping
Sultana et al. 2017	MANET	AOMDV and ECC	Communication security	Blackhole
Ramesh et al. 2019	WSN	Trust-based decision making	Packet loss, dependability, energy consumption, end to end delay, and resilience.	Sinkhole and Blackhole
Alshehri et al. (2019)	IoT-WSN	Fuzzy logic based attack detection	Average trust score analysis	Malicious nodes
Selvi et al. (2019)	Mobile WSN	Trust-score analysis	Security, energy-efficiency, and Packet Delivery Ratio (PDR)	Malicious nodes
Mahantesh et al. (2020)	WSN	Trust and reputation-based reliable relay selection	Number of alive nodes, battery power factor, and Time	Malicious node

Yu et al. (2020)	WSN	Trust and cryptography-based protocol	Average remaining energy and security analysis	No impersonation and Man-in-middle attack
Kore et al. (2020)	IoT-WSN	Cross-layer trust computation	Throughput, PDR, energy consumption, and communication overhead	Man-in-middle attack
Poomagal et al. (2020)	Internet of Vehicles (IoV)	ECC-based secure data transmission	Computation cost and communication overhead	Stolen verifier attack, insider attack, man-in-middle attack, guessing attack, and impersonation attack.
Ali et al. (2020)	WSN	Modified Diffie–Hellman method	Computational time, encryption time, key generation time, and decryption time	Plaintext attack, related key attack, and man-in-middle attack
AlMajed et al. (2020)	IoT-WSN	ECC-based secure data transmission	Complexity analysis, number of rounds, enhancement, processing utilization, space utilization, and energy consumption	Chosen plain text attack, cipher text attack, and chosen cipher text attack
Chaitra et al. (2021)	WSN	Multi-objective function for clustering and ECC for security	Throughput, energy consumption, and security analysis	Malicious attacks

Table 1 demonstrates the comparative study of all the recent security solutions to protect the wireless networks (WSN, IoT, MANET, etc.) in terms of methodology, performance parameters, attacks, etc. The security methods include the trust-based, cryptography-based, and combination of both trust-based and cryptography-based methods. The SRAMI work proposed in this paper by considering the AMI system requirements of security. Designing wireless communication security for AMI is the basic need in the electricity sector to make the smart grid. AMI worsens the performance because of no security provisions for AMI. Hence, SRAMI proposed to address the concerns of reliability and security for data transmission operations in a WSN-assisted AMI network.

B. Trust Management for Communication Infrastructure

Trust management in communication infrastructure becomes essentials for reliable data transmissions. Some recent works introduced by considering the real-time communication infrastructure. AMI communication infrastructure, designing factors should be logical, which gives faithful end to end delivery. Some of the parameters are Network topology design, secure routing protocol, secure forwarding, end to end communication, secure broadcasting, and DoS defense. For any wireless network, the selection of a trusted node is one of the vital tasks [Mahajan et al. 2020]. In this paper, we proposed WSN for wireless communication to AMI and its result increases sensor nodes to transfer the information from one place to another place. Secure selection of sensor node performs according to the trust-evaluation algorithm. Table 2 presents the literature review of some trust-based algorithm for security improvement of communication infrastructure. The trust management algo-

rithm investigated using performance parameters such as network life, communication cost, energy consumption, the efficiency of a network, overhead, security of routing, PDR, data integrity, and, reliability. Trust-based schemes were applied on various wireless networks to enhance routing performance [Mahajan et al. 2020].

Table 2. State-of-the-art of trust-based schemes for communication infrastructure

References	**Trust based scheme**	**Considered technology**	**Advantages**
Adnane et al. (2013)	OLSR	Ad hoc network	1.efficiency of the network increases
Amin et al. (2018)	BAN logic	WSN	1.Efficient and robust
Latha et al. (2019)	TA-EEA scheme	WSN	1.Minimizes energy usage 2.Minimum overhead 3.High PDR
Alqahtani et al. (2020)	Trust based monitoring scheme	IOT	1.Communication cost reduced 2. Network life increased 3. Energy consumption reduced
Rouissi et al. (2019)	LEACH scheme	WSN	1.Data integrity good 2.Energy efficiency good 3.High reliability 4.Secure routing
Mahajan et al. (2020)	CL-IoT	IoT for Precision agriculture	1. Cross layer parameters computed 2. Optimal cluster head selection 3. Reduced energy consumption 4. Reduced computation cost 5. Improved QoS performance
Moghadam et al. (2020)	IEC 62351	Communication infrastructure	1.Overcome security weaknesses 2.Communication cost reduces 3.Minimizes overhead

The performance of the routing method is based on a reliable path discovery. And finding the trusted path is based on the trust evaluation algorithm. The Internet of Things (IoT) supports smart systems and its wireless communication based on WSN. Trust monitoring scheme reduces the communication cost, minimizes overhead, and increases the network life. Correspondingly, the logic of the OLSR protocol was used for trust management schemes in routing. None of the existing works re-designed or considered for the infrastructure of AMI communications. For AMI deployment, we are focusing on two concerns in this paper such as security and energy-efficiency. The reliability of communicating the periodic electric meter readings with the intended recipient and the security of protecting sensitive data from the various vulnerable threats are important goals for a smart AMI system.

C. Research motivations and Contributions

The State-of-the-art shows that wireless communication security is a big issue in IoT enabled smart systems. The problem becomes challenging for smart AMI systems. DoS attack, malicious attack, black hole attack, and man in the middle attack collapse the system and eventually, Smart Grid (SG) degrades the performance. AMI is a part of SG, and we can save electricity by providing security for the com-

munication infrastructure of AMI. Ultimately, SG enhances performance. In short, the key requirement of AMI systems is the securities from the various attacks in wireless communications such as WI-FI/WLAN networks. In general, the cybersecurity requirements of AMI include confidentiality, integrity, availability, etc. that can be vulnerable to wireless security threats during wireless communications. This work motivates by providing a reliable and secure path in the routing of WSN called SRAMI. Communication infrastructure is the main element of AMI. Consequently, through reliable and secure communication infrastructure to AMI, the present work is to support and develop the SG of the electricity sector.
The contributions are:

- Optimizing the AMI system by providing the smart communication protocol at the network layer supports reliable route discovery and a lightweight security algorithm for the transmission of electrical data.
- For reliable route discovery, we used the trust-based approach to select the next relay node for data transmission. In trust-computation, each AMI node is analyzed by computing its trust score using the trust parameters mentioned in figure 1.
- For secure data transmission, the lightweight cryptography algorithm is designed that depends on the efficient key management technique, data encryption, and its verification at each intermediate AMI node. The proposed protocol SRAMI is more effective than the above-stated protocols in the state-of-the-art. SRAMI mainly focused on finding a reliable path of communication and the security algorithm works to provide security on a reliable path.
- The SRAMI protocol simulated and evaluated with state-of-art protocols by considering the different network conditions in terms of parameters mentioned in figure 1.

3 Proposed Methodology

A. System Design and Assumptions

This section presents the complete design of the proposed SRAMI protocol to address the significant requirements for the calculation process of the reliable path using trust parameters such as energy, geographical distance, and bandwidth and cryptography-based secure data transmission. Figure 2 demonstrates the AMI design considered in this paper. As showing in figure 2, the AMI system consists of T number of AMI nodes $\{A^1, A^2, \dots A^T\}$ called smart meters deployed at edge layer randomly in area of size $X \times Y$. The data collected by AMI nodes transmitted to corresponding local gateway nodes and then to destination node D called utility node via intermediate relay AMI nodes. Figure 2 also demonstrates that how each smart meter connected to various electric equipments such as fridge, television (TV), bulbs, etc.

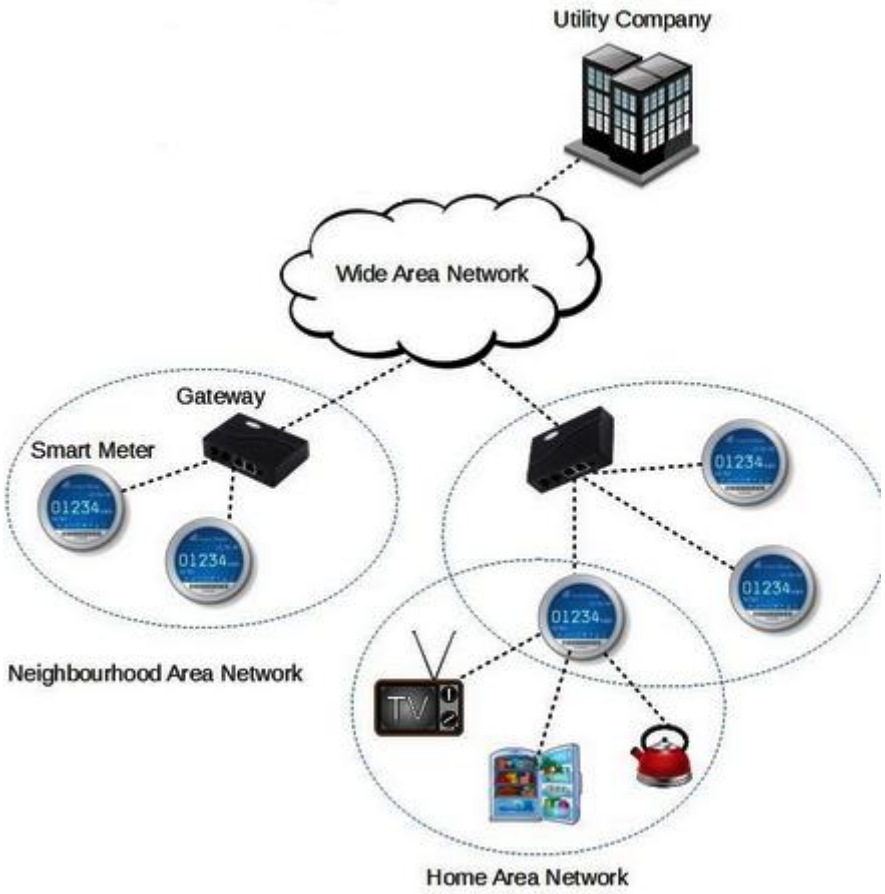

Figure 2. Structure of AMI system

The design of AMI systems based on assumptions such as:

- All the AMI nodes are equipped with the functionality of periodical meter reading of electricity consumptions of all connected devices. In short, such smart meter nodes act as the sensing node that periodically senses the electricity data reading and transmitting towards the utility node.
- The AMI nodes are constrained by processing capabilities and processing power.
- The utility node is outside of the network without any resource constraint.
- The malicious nodes are part of the AMI network that performs the malicious activities by spreading false information among the neighboring AMI nodes.
- The data from source AMI node to destination utility node transmitting in a multi-hop manner.

B. SRAMI Design

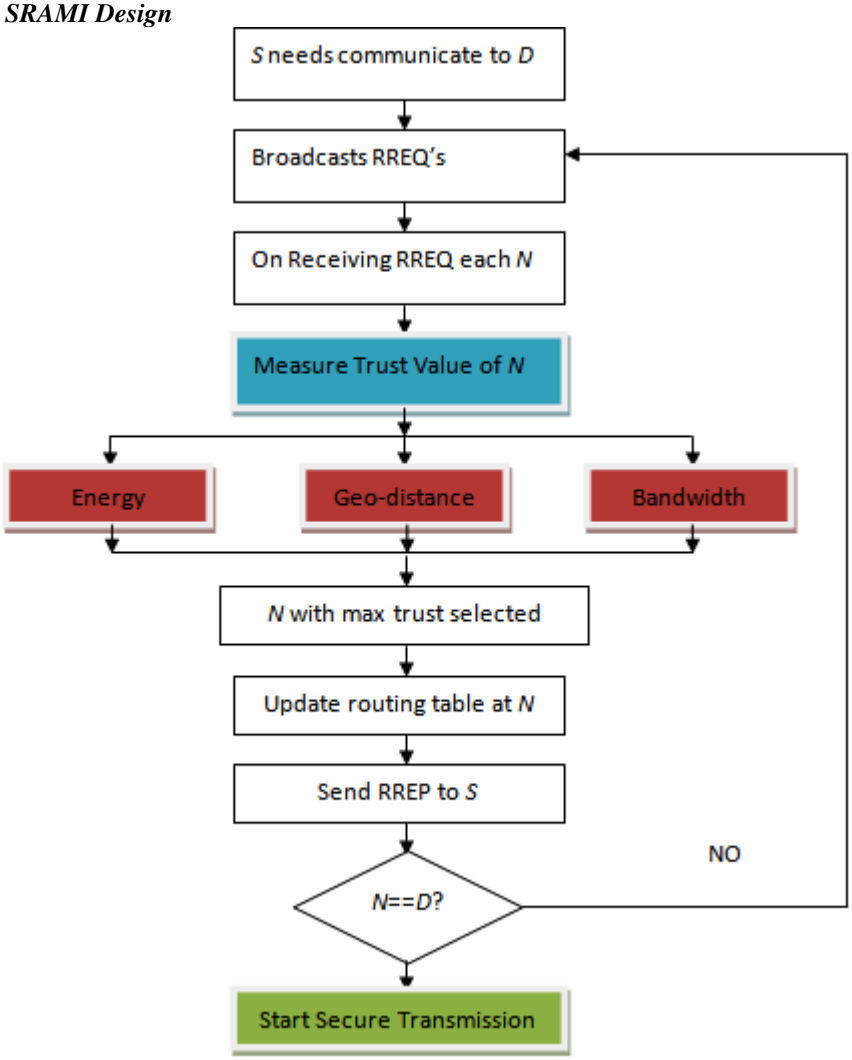

Figure 3. Design of proposed SRAMI protocol for smart AMI system

As per the above system design and assumptions, we proposed SRAMI protocol to address the challenges of reliable and secure data transmissions under cyber threats. SRAMI algorithm goes to provides reliable and secure communication. As per the problem statement, we prepared the below network design parameters for the evaluations of different routing methods for AMI network security. SRAMI algorithm proposed to enhance the performance of SG than the way of suggested literature survey schemes for reliable and secure communication. Batch rekeying operations tried to provide secure communication for AMI by using key management schemes [Benmalek et al. 2018], but it failed to provide reliable communications.

I. Reliable Route Discovery

As observe in figure 3, after the AMI network deployment with a group of sensor nodes and utility node, the reactive route construction process starts by any source node S in the network by generating and spreading Route Request packets near the actual receiver node D. RREQs are broadcasted to all the sensors within the near to S as per demand to search the trustworthy and a reliable route. All the neighbors of node source or current intermediate node are recorded into the set N_i^D(set of all neighbors of node i towards endpoint or receiver D (Utility node)). Thus, the path as of existing node i to succeeding node j is constructed by computing the trust score of each neighboring node of node i. The three most important parameters are calculated for finding a trust-based routing path. The parameters are such as energy capabilities, bandwidth capabilities, and geographic distance between i^{th}sensor nodes to Utility node (D) in the AMI network. The computed values of each neighboring node are considered as the trust value and at each session, it can be updated in the routing-table. Once the RREQs received by neighboring nodes, then the probability is computed as:

$$T_j^i = E_j + G_{ij} + B_j \quad (1)$$

Where, the T_j^i is the trust value of node j for becoming the relay of node i. The E_j and B_j is the energy capabilities and bandwidth capabilities of node j. As the sensor nodes are fixed position, our aim is to select the path with minimum geographic distance from S to D. G_{ij} is the geographic distance from node $i^{th}$to j^{th}node.

The conditions for energy and bandwidth at each node are evaluated as: The calculations of energy consumption founded to next hop selection are below three equations:

$$R_{node} - E_{needed} > \varepsilon, then\ E_j = 1 \quad (2)$$

$$R_{node} - E_{needed} = \varepsilon, then\ E_j = 0 \quad (3)$$

$$R_{node} - E_{needed} < \varepsilon, then\ E_j = -1 \quad (4)$$

Where R_{node}enduring energy of succeeding hop, E_{needed} is essential energy to spread the current data and ε is threshold to satisfy. If the equation 2 satisfied then E_j is trust value set to true from current node i to next node j. Else if equation 4 is satisfied then E_j trust value is set to false from current node i to next node j. Otherwise in rare case, trust value is set to 0. This helps to improve reliability through selecting the more stable path for the reliable data transmission. Similarly, the bandwidth is evaluated as:

$$O_{node} + B_{needed} < \sigma, then\ B_j = 1 \quad (5)$$

$$O_{node} + B_{needed} = \sigma, then\ B_j = 0 \quad (6)$$

$$O_{node} + B_{needed} > \sigma, then\ B_j = -1 \quad (7)$$

Where O_{node} bandwidth occupancy at the current node, B_{needed} is vital bandwidth to convey the recent data and σ is the lower bandwidth limit to satisfy. Geographical the distance from node i to next node j measured as:

$$G_{ij} = \frac{750 - \left(N_{xy}^i - N_{xy}^j\right)}{750} \quad (8)$$

Where, N_{xy}^i & N_{xy}^j is the location value N_{xy} of node i and j. The j node is by default the destination node. We considered the maximum distance between two

nodes in 750 meters. We received the distance trust value in the range of 0 to 1. The maximum the distance trust value, the better probability of the node to select. The proposed approach is its simple and having minimum overhead of discovering the reliable route. These all equations utilized in algorithm 1 for reliable route discovery in SRAMI protocol.

Algorithm 1: Trust-based reliable route discovery

Inputs

S: $Source\ node$
D: $Destination\ node\ (Utility\ node)$
RT: $Routing\ table$
ε: $energy\ threshold$
σ: $lower\ bandwidth\ limit$

Output

1. S discovers the one-hop neighbouring vehicles n
2. S broadcast RREQ's to n
3. Upon receiving RREQ at each $R \epsilon n$
   $\delta 1 = energy\ (R)$ using Eq. (2-4)
   $\delta 2 = bandwidth\ (R)$ using Eq. (5-7)
   $\delta 3 = geodist\ (R, D)$ using Eq. (8)
4. Compute the trust value for each $R \epsilon n$
   $P^R = \delta 1 + \delta 2 + \delta 3$
5. Select *forward node* R with max value P^R among all n
6. Update routing value in routing table RT
7. R sends RREP to S
8. If $(R == D)$
9. Secure data transmission from S to D (apply algorithm 2)
10. Else
11. Go to step 2
12. End If
13. STOP

II. Secure Data Transmission

After discovering the reliable route to start data transmission from source node to destination node, we designed lightweight cryptography approach with effective key management technique. Algorithm 2 shows the processing of sending the data from source to destination node using Elliptic Curve Cryptography (ECC). The ECC is a recent technique introduced as an alternative to Rivest–Shamir–Adleman (RSA) cryptography. ECC provides security among the key pairs using the elliptic curves mathematics. In RSA, a similar kind of approach adopted using prime numbers rather than elliptic curves. ECC gained significant attention recently due to strong security with small key sizes. ECC depends on the structure of elliptic curves for public-key cryptography operations and hence its keys remain very difficult to crack. Due to the security and computational efficiency using ECC, we designed

cryptography functions to transmit the electric data from AMI node to intended utility node in algorithm 2. This algorithm not only achieves the data security but also achieves the user privacy preservation.

Algorithm 2: Secure Data Transmission

Inputs

S: $source\ node$
D: $destination\ node$
IN: $current\ intermediate\ node$
Kpu: $Public\ key$
$Kgpu$: $Group\ private\ key$
Kpr: $Private\ key$
Kss: $Session\ key$
P: $current\ packet$

1. Key Generation
   1.1 Key generation via broadcasting $ID\ of\ S$
   1.2 Extract the Kpu, Kpr, Kss
   1.3 $Kgpu = Kpr \times Kss$
   1.4 Update routing table
2. $At\ S\ Node$
   2.1 Fetch routing information
   2.2 Get current Kss
   2.3 Generate new Kss
   2.4 Updated routing table with new key
   2.5 Apply key ECC encryption at IM and D using Kpu, Kpr
   2.6 Signing by S using $Kgpu$
   2.7 Transmit current P towards next hop IM
3. $At\ IN\ Node$
   3.1 $Success = verify\ (P)$ using $Kgpu$
   3.2 IF ($Success == true$)
   3.3 IF ($IN == D$)
   3.4 Decrypt current packet using $Kgpu$
   3.5 Send ACK
   3.6 ELSE
   3.7 Signing received packet and forward to next IN in selected path using set of keys
   3.8 END IF
   3.9 ELSE
   3.10 Packet is received from malicious node
   3.11 $Drop\ (P)$
   3.12 END IF
4. STOP

As demonstrated in algorithm 2, the group of keys generated using ECC key generation technique. The private key Kpr is randomly generated. The Kpu is generated

by the elliptic curve parameter. The session key Kss is generated by using the current session ID for appropriate key management in network as well as protecting the communications. To improve the security further, the group private key $Kgpu$ is generated using the public and current session key. The group private key is used for generating the digital signature of encrypted data and its verification. The key size selected for all is 256 bits (which is very small compared to conventional mechanisms) with high-security provisions. As the ECC technique does not provide in-built encryption and decryption capabilities, we combined this approach with the Advanced Encryption Standard (AES-128). AES-128 encrypts and decrypts the electric data from smart meters using the set of keys generated using ECC.

4 Simulation Results and Discussions

The selection of a reliable and secure path of routing in WSN ended with the SRAMI algorithm. The simulation is possible with the help of NS2 as it evaluates the proposed protocol with exiting protocols following QoS parameters compared. The proposed SRAMI algorithm is evaluated by choosing a random and grid type of topology [Halle et al. 2020]. As the AMI network deployed randomly or grid type, we designed the networks of both scenarios with the number of AMI nodes. Tables 1 and 2 show the set of simulation parameters for random and grid network topologies respectively. In a random network scenario, a varying number of AMI nodes were deployed to verify the scalability and reliability of the SRAMI protocol with a fixed data rate of 20 packets/second. In grid topology, we designed a grid network of 25 AMI nodes with varying data rates in the range of 10 packets/second to 50 packets/second. In both scenarios, we introduced the presence of 10 % malicious attackers. The performance of SRAMI protocol compared with two conventional non-secure protocols AODV and DSDV, and two secure protocols such as AASR (cryptography-based) [Liu et al. 2014] and TERP (trust-based) [Shen et al. 2017]. We selected AASR and TERP protocols for comparative study, as our goal to claim the efficiency of using the hybrid approach in SRAMI protocol with the minimum computational burden. For comparative analysis, we computed the five well-known parameters such as average throughput, Packet Delivery Ratio (PDR), delay, overhead, and energy consumption. Figure 4 shows the examples of both scenarios that demonstrate the deployed topologies and communications among the AMI nodes and utility nodes in presence of malicious nodes (red-colored).

Table 1. Random AMI topology simulation parameters

Smart Meters / AMI nodes	10-60
Data Collector nodes	2
Utility node	1
Malicious nodes	10 %

MAC layer	802.11
Topology	Random waypoint mobility
Nodes position	Static
Packet size	512 bytes
Traffic pattern	Constant Bit Ratio (CBR)
Number of connections	5
Simulation time	350 seconds
Data rate	20 packets/second

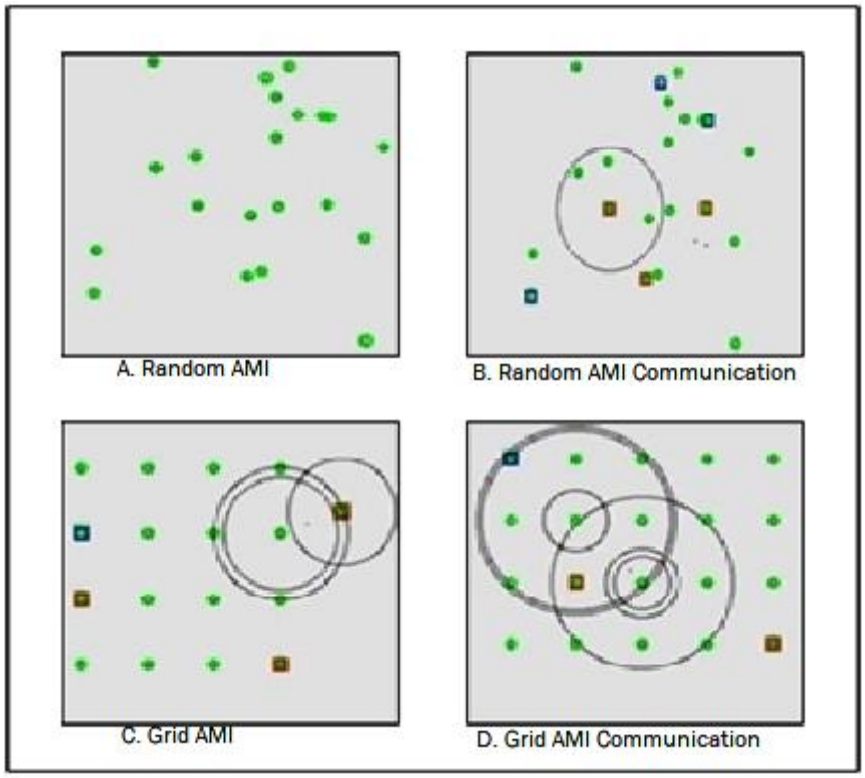

Figure 4. Visual representation of random and grid AMI networks and communications

Table 2. Grid AMI topology simulation parameters

Smart Meters / AMI nodes	25
Data Collector nodes	2

Utility node	1
Malicious nodes	10 %
MAC layer	802.11
Topology	Grid mobility
Nodes position	Static
Packet size	512 bytes
Traffic pattern	Constant Bit Ratio (CBR)
Number of connections	5
Simulation time	350 seconds
Data rate	10-50 packets/second

A. Random AMIs Evaluation

In random topology, we varied the smart meters density from 10 to 60. Figures 5-9 demonstrate the comparative results for parameters average throughput, PDR, delay, overhead, and energy consumption respectively. Figure 4 demonstrates the outcome of average throughput for a varying number of smart meters. The conventional routing protocols AODV and DSDV have poor throughput results compared to other protocols as they do not have provisions to defend against the malicious nodes in the network. Among other secure protocols, SRAMI improved the throughput performance compared to AASR and TERP protocols due to the provision of establishing the trust-aware route and lightweight cryptography-based data security.

Figure 6 showing the PDR outcomes that overlapping the trend of throughput results. As the number of smart meters increases, the performance of throughput and PDR decreases significantly. It is mainly because of an increasing number of malicious nodes in the network and long-distance communications. Among all the protocols SRAMI leads to significant improvement in PDR performances as minimizes the number of link break probabilities due to malicious users and protects the data from being compromised. It also impacts communication delay performances (figure 7) for SRAMI protocol compared to other protocols. As the frequent route discovery and re-transmissions are reduced in the SRAMI protocol, it significantly reduces the communication delay as well. In some networks, the non-secure protocol (AODV & DSDV) shows the minimum communication delay compared to secured protocols (AASR & TERP). It is because of extra provisioning provided in AASR and TERP protocols to defend against the malicious nodes. However, the QoS (throughput & PDR) of AODV and DSDV protocols degraded badly due to malicious nodes.

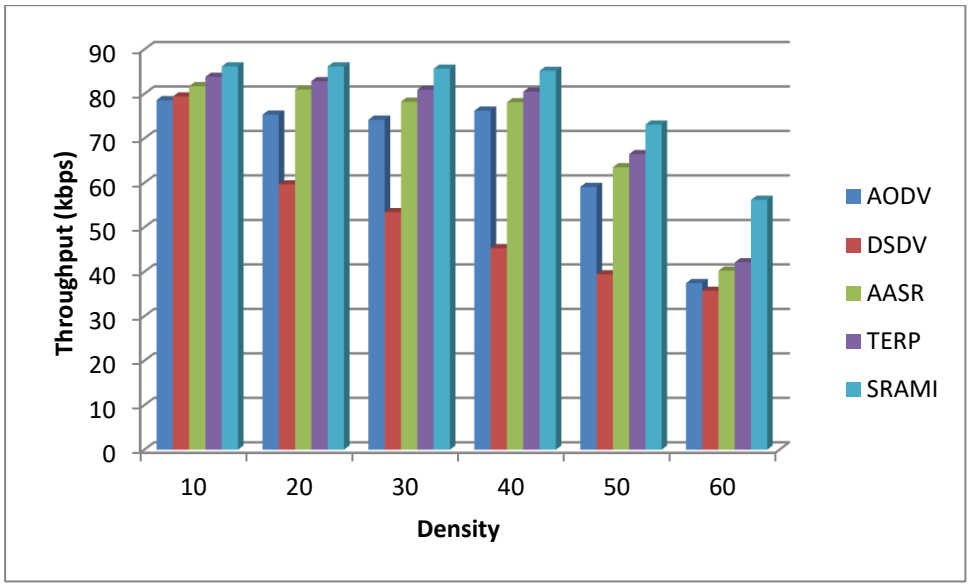

Figure 5. Performance analysis of average throughput for random topology

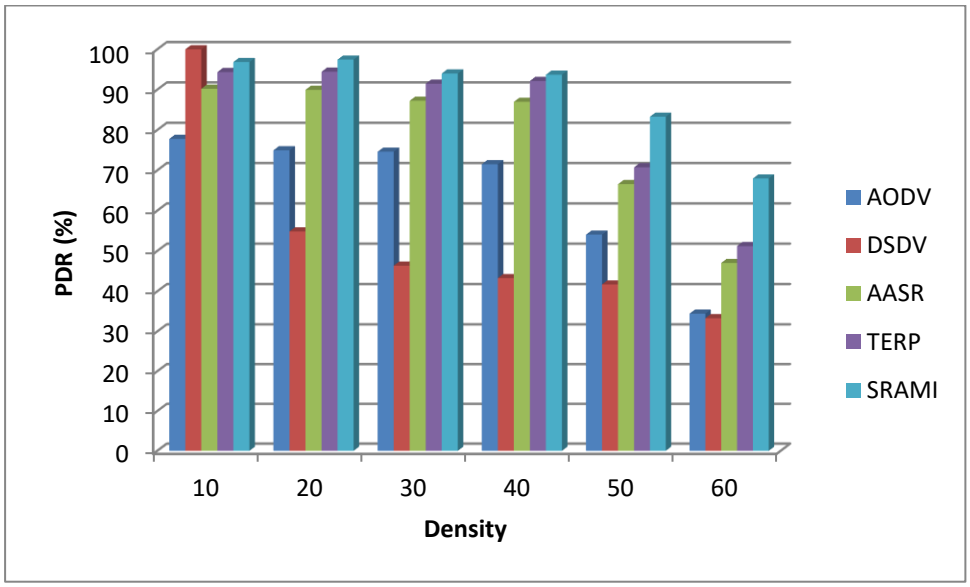

Figure 6. Performance analysis of PDR for random topology

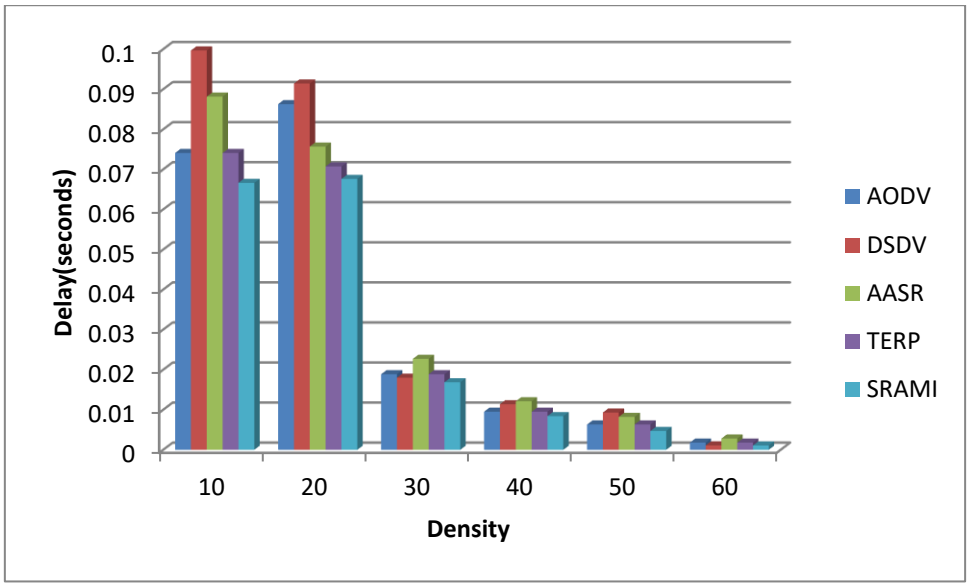

Figure 7. Performance analysis of Delay for random topology

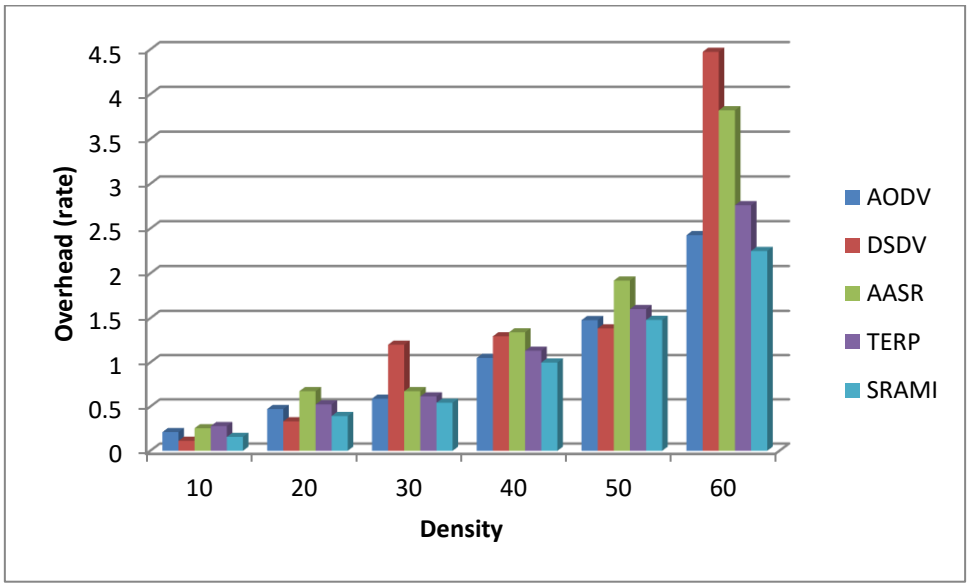

Figure 8. Performance analysis of overhead for random topology

Figure 8 demonstrates another important performance metrics for network-layer protocols. The communication overhead is mainly caused by frequent re-transmissions, route discovery functions, and other routing tasks. The SRAMI

protocol minimizes such frequent re-transmissions, route discovery, and routing functions by providing a reliable and secure methodology for smart AMI networks. The SRAMI protocol able to reduce the communication overhead compared to trust-based and cryptography-based protocols. The reduction in parameters like delay and overhead directly affects the energy consumption performance as well. Figure 9 shows the outcome of average energy consumption results for all the protocols. The SRAMI protocol minimizes the average energy consumption for each AMI network compared to other protocols; hence, it improves the network lifetime performance.

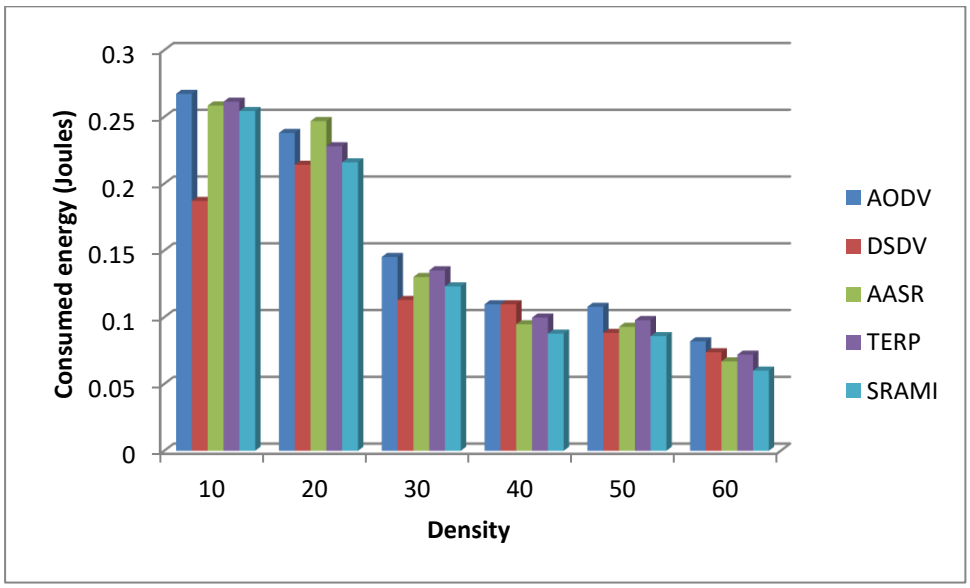

Figure 9. Performance analysis of average energy consumed for random topology

B. Grid AMI Evaluations

This section presents the simulation results for grid topology with the varying data rate. The purpose of grid AMI designing is to consider the real-time deployment of smart meters for each home. In rural or semi-urban areas of India, housing societies in a grid manner where there is the possibility of electricity theft. By deploying the smart meters in such regions, the electricity theft probability can be neutralized. However, wireless threats may introduce challenges for managing the SG effectively. The result in figures 10-14 demonstrates the outcome of throughput, PDR, delay, overhead, and energy consumption respectively. The data rate variations investigated with grid topology of AMI networks. The higher data rate introduces a higher communication burden, communication delay, and communication overhead for AMI networks.

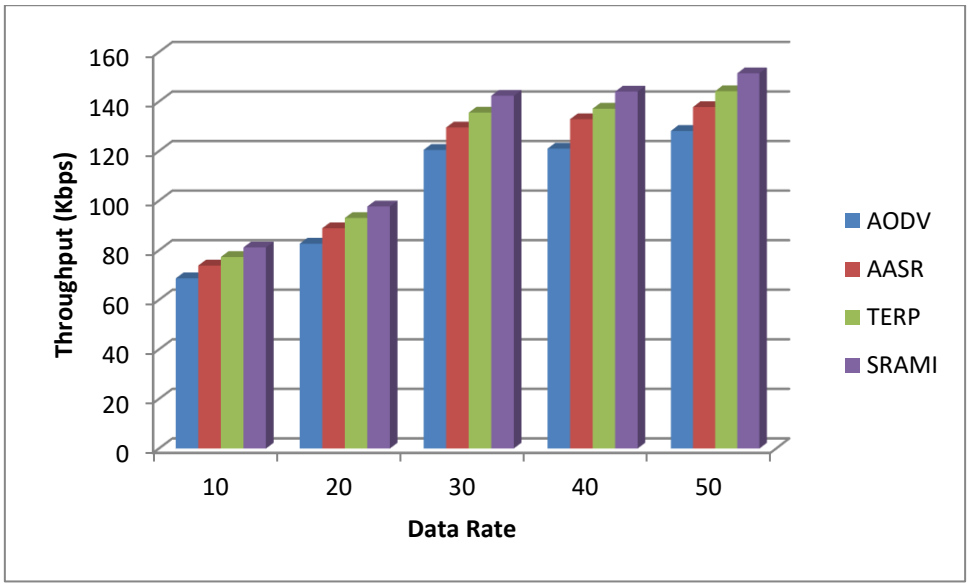

Figure 10. Performance analysis of average throughput for grid AMI network

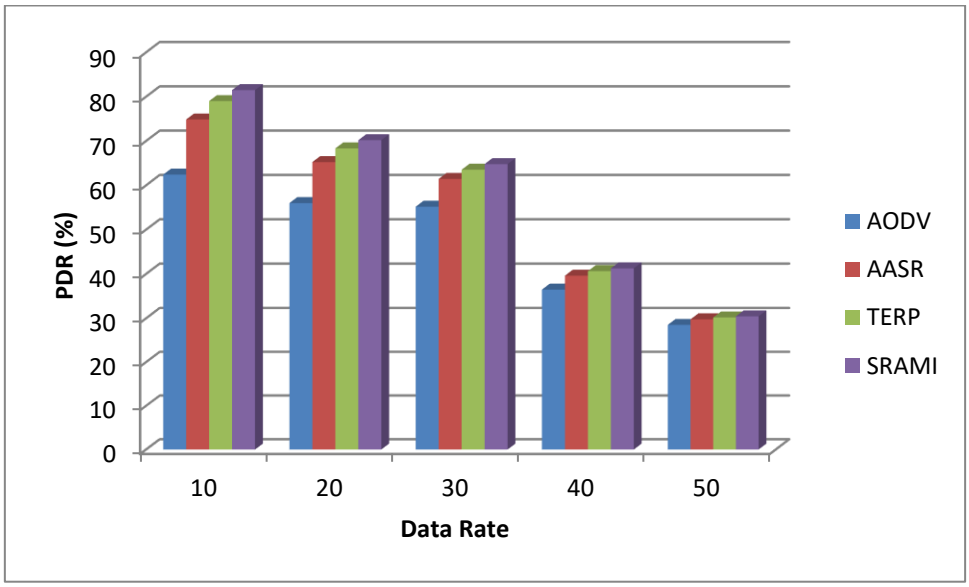

Figure 11. Performance analysis of PDR for grid AMI network

Figure 10 demonstrates the average throughput performances with varying data rates. It shows that the increase in data rate increases the throughput for all the protocols because the rate packets generated increase per second. The performance

of SRAMI shows the promising among all the secured and non-secured protocols. Among the cryptography-based (AASR) and trust-based (TERP) protocols, the latter one has a high throughput performance and PDR (figure 11) performances (by considering random and grid topologies). TERP focused on establishing more reliable routes without data security and AASR focused on data security without reliable routes. In both cases, complete protection against malicious attackers cannot be achieved. The PDR results show that increasing data leads to increasing packets dropped in the network.

The communication delay shows in figure 12 concerning an increasing number of data rates. The communication delay has increased significantly since after 30 packets/second data rate as it increasing the significant congestions on transmission links. The SRAMI protocol able to keep minimum delay in all cases compared to all the protocols. A similar reflection was noticed for communication overhead (figure 13) as well. The AASR protocol shows high computation overhead compared to the TERP protocol due to cryptography operations. The SRAMI protocol reduces communication overhead because of a reduction in re-transmissions and routes discovery operations compared to AASR and TERP protocol. The average energy consumption performance in figure 14 demonstrates no fluctuations with a varying data rate as the fixed number of smart meters in the network. The proposed one reduced the energy consumption performance significantly compared to all the protocols.

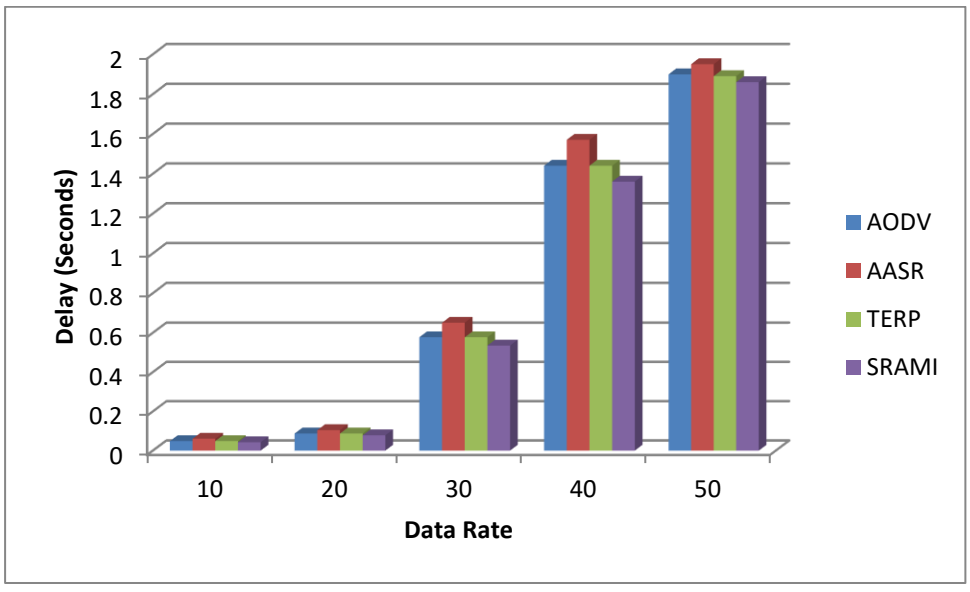

Figure 12. Performance analysis of delay for grid AMI network

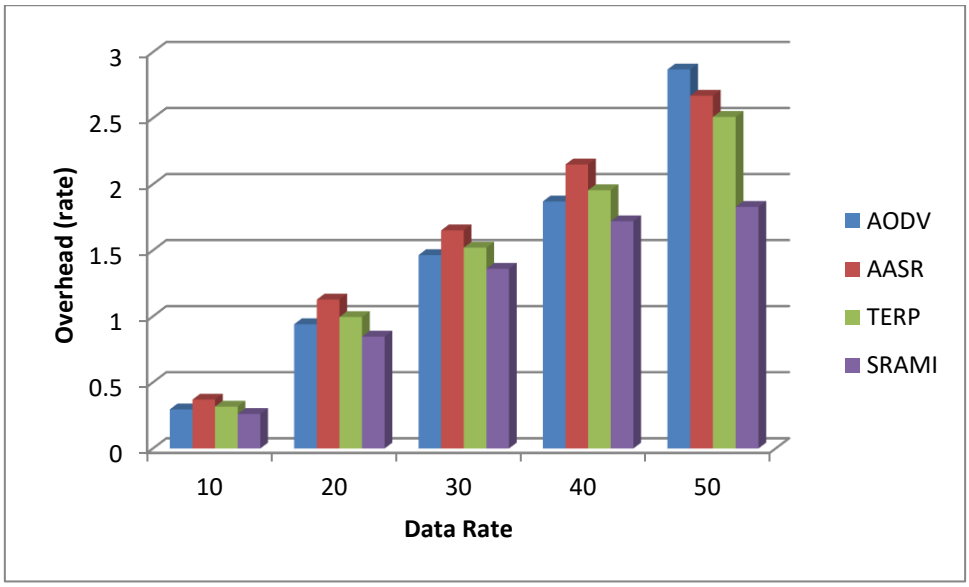

Figure 13. Performance analysis of overhead for grid AMI network

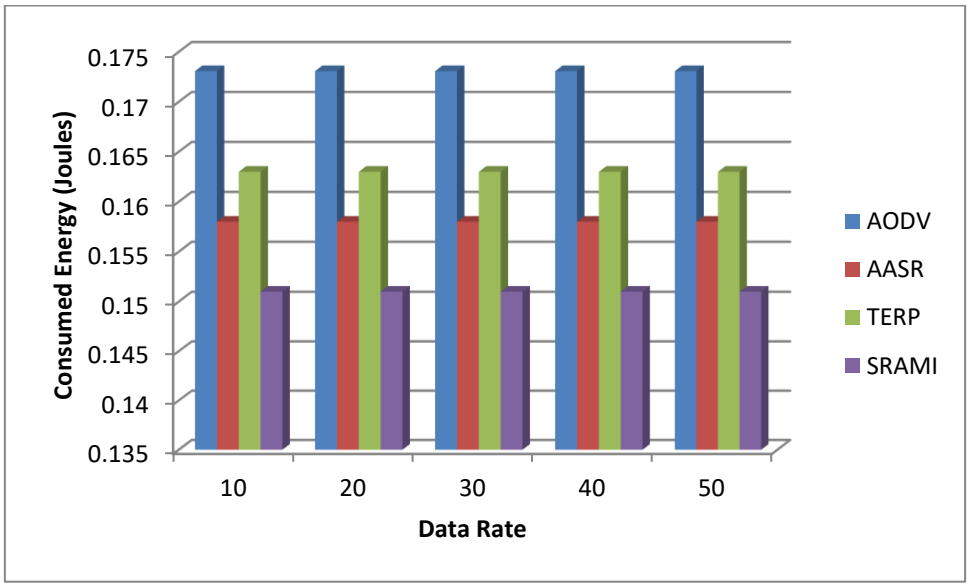

Figure 14. Performance analysis of average consumed energy for grid AMI network

5 Conclusion and Future Work

A variety of security-related challenges occurs in AMI therefore introduced SRAMI algorithm with the purpose to mitigate reliability and data security issues. A combination of trust-based and lightweight cryptography-based SRAMI algorithm improved the security and reliability of AMI. For route discovery, we designed an effective and simple trust model to select a reliable relay node using the three trust parameters. For secure data transmission, we designed an ECC-based cryptography technique combined with the AES-128 method. The supersite of the ECC-based mechanism is small key sizes with high security for smart AMI communications. The simulation results show that TERP has more advantages in the requisites of energy efficiency in communication. The decision is based on the performance of Throughput, delay, PDR, overhead, and energy consumption. Our present structure shows an intellectual conclusion for wireless communication routing for smart AMI by decreasing the ratio of energy consumption, delay, and overhead with the enhanced throughout and PDR compared to existing secured and non-secure protocols. Ultimately, SRAMI supports the electricity sector and tried to save electricity. In future work, we suggest scrutinizing the recital of the projected structure should be more secure and reliable by reducing the cost factor and complexity of wireless communication infrastructure to AMI. Secure wireless communication infrastructure is a big challenge of AMI. To redesign lightweight and simple algorithms for secure wireless communication infrastructure to AMI needed in the future.

Compliance with Ethical Standards:

Funding: No Funding.

Conflict of Interest: All authors declares that they has no conflict of interest.

Ethical approval: This article does not contain any studies with human participants performed by any of the authors.

References

Al-Turjman, F., & Abujubbeh, M. (2019). IoT-enabled smart grid via SM: An overview. Future Generation Computer Systems. doi:10.1016/j.future.2019.02.012.

Adnane A, Bidan C, de Sousa Júnior R (2013) Trust-based security for the OLSR routing protocol. Computer Communications 36:1159-1171. doi: 10.1016/j.comcom.2013.04.003

Alqahtani F, Al-Makhadmeh Z, Tolba A, Said O (2020) TBM: A trust-based monitoring security scheme to improve the service authentication in the In-

ternet of Things communications. Computer Communications 150:216-225. doi: 10.1016/j.comcom.2019.11.030

Amin R, Hafizul Islam S, Biswas G, Obaidat M (2018) A robust mutual authentication protocol for WSN with multiple base-stations. Ad Hoc Networks 75-76:1-18. doi: 10.1016/j.adhoc.2018.03.007.

Alshehri, M.D., Hussain, F.K. A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT). Computing 101, 791–818 (2019). https://doi.org/10.1007/s00607-018-0685-7.

Ali, S., Humaria, A., Ramzan, M. S., Khan, I., Saqlain, S. M., Ghani, A., … Alzahrani, B. A. (2020). An efficient cryptographic technique using modified Diffie–Hellman in wireless sensor networks. International Journal of Distributed Sensor Networks, 16(6), 155014772092577. doi:10.1177/1550147720925772.

AlMajed, Hisham & Al-Mogren, A.s. (2020). A Secure and Efficient ECC-Based Scheme for Edge Computing and Internet of Things. Sensors. 20. 6158. 10.3390/s20216158.

Barsana Banu J., Jeyashanthi J., Thameem Ansari A., Sathish A. (2021) Development and Implementation of the Smart Energy Monitoring System Based on IoT. In: Zhou N., Hemamalini S. (eds) Advances in Smart Grid Technology. Lecture Notes in Electrical Engineering, vol 688. Springer, Singapore. http://doi-org-443.webvpn.fjmu.edu.cn/10.1007/978-981-15-7241-8_38.

Baroudi U, Bin-Yahya M, Alshammari M, Yaqoub U (2018) Ticket-based QoS routing optimization using genetic algorithm for WSN applications in smart grid. Journal of Ambient Intelligence and Humanized Computing 10:1325-1338. doi: 10.1007/s12652-018-0906-0

Benmalek M, Challal Y, Derhab A, Bouabdallah A (2018) VerSAMI: Versatile and Scalable key management for Smart Grid AMI systems. Computer Networks 132:161-179. doi: 10.1016/j.comnet.2018.01.010.

Chaitra H.V., RaviKumar G.K. (2021) Secure and Energy-Efficient Data Transmission. In: Chiplunkar N., Fukao T. (eds) Advances in Artificial Intelligence and Data Engineering. Advances in Intelligent Systems and Computing, vol 1133. Springer, Singapore. https://doi.org/10.1007/978-981-15-3514-7_98.

Das, A., & Islam, M. M. (2012). SecuredTrust: A Dynamic Trust Computation Model for Secured Communication in Multiagent Systems. IEEE Transactions on Dependable and Secure Computing, 9(2), 261–274. doi:10.1109/tdsc.2011.57.

Fadlullah, Z.M., Pathan, AS.K. & Singh, K. Smart Grid Internet of Things. Mobile Netw Appl 23, 879–880 (2018). https://doi.org/10.1007/s11036-017-0954-2

Halle P, Shiyamala S (2020) Trust and Cryptography Centered Privileged Routing Providing Reliability for WSN Considering Dos Attack Designed for AMI of Smart Grid. International Journal of Innovative Technology and Exploring Engineering 9:1794-1800. doi: 10.35940/ijitee.b7449.019320

Kraounakis S, Demetropoulos I, Michalas A, Obaidat M, Sarigiannidis P, Louta M (2015) A Robust Reputation-Based Computational Model for Trust Establishment in Pervasive Systems. IEEE Systems Journal 9:878-891. doi: 10.1109/jsyst.2014.2345912.

Kore, A., Patil, S. IC-MADS: IoT Enabled Cross Layer Man-in-Middle At-

tack Detection System for Smart Healthcare Application. Wireless Pers Commun 113, 727–746 (2020). https://doi.org/10.1007/s11277-020-07250-0.

Latha A, Prasanna S, Hemalatha S, Sivakumar B (2019) A harmonized trust assisted energy efficient data aggregation scheme for distributed sensor networks. Cognitive Systems Research 56:14-22. doi: 10.1016/j.cogsys.2018.11.006

Lekshmi S, Sivraj P, Sasi K (2020) Selection of routing protocols for advanced metering infrastructure. In: Semanticscholar.org. https://www.semanticscholar.org/paper/Selection-of-routing-protocols-for-advanced-Lekshmi-Sivraj/c5e0ecf6e31d76ffd187620af424e3ab488ff4c6.

Liu, W., & Yu, M. (2014). AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments. IEEE Transactions on Vehicular Technology, 63(9), 4585–4593. doi:10.1109/tvt.2014.2313180.

Mahajan, H.B., & Badarla, A. (2018). Application of Internet of Things for Smart Precision Farming: Solutions and Challenges. International Journal of Advanced Science and Technology, Vol. Dec. 2018, PP. 37-45.

Mahajan, H.B., Badarla, A. & Junnarkar, A.A. (2020). CL-IoT: cross-layer Internet of Things protocol for intelligent manufacturing of smart farming. J Ambient Intell Human Comput. https://doi.org/10.1007/s12652-020-02502-0.

Mathapati, M., Kumaran, T.S., Muruganandham, A. et al. Secure routing scheme with multi-dimensional trust evaluation for wireless sensor network. J Ambient Intell Human Comput (2020). https://doi.org/10.1007/s12652-020-02169-7.

Huh, JH., Otgonchimeg, S. & Seo, K. Advanced metering infrastructure design and test bed experiment using intelligent agents: focusing on the PLC network base technology for Smart Grid system. J Supercomput 72, 1862–1877 (2016). https://doi.org/10.1007/s11227-016-1672-4.

Moghadam M, Nikooghadam M, Mohajerzadeh A, Movali B (2020) A lightweight key management protocol for secure communication in smart grids. Electric Power Systems Research 178:106024. doi: 10.1016/j.epsr.2019.106024.

Muhanji S.O., Flint A.E., Farid A.M. (2019) The Development of IoT Within Energy Infrastructure. In: eIoT. Springer, Cham. https://doi.org/10.1007/978-3-030-10427-6_3.

N C, Basit A, Singh P, V. Ch V (2018) Lightweight Cryptography for Distributed PKI Based MANETS. International journal of Computer Networks & Communications 10:69-83. doi: 10.5121/ijcnc.2018.10207

Ou, W., Wang, X., Han, W., & Wang, Y. (2009). Research on Trust Evaluation Model Based on TPM. 2009 Fourth International Conference on Frontier of Computer Science and Technology. doi:10.1109/fcst.2009.10.

Pavithira L (2016) A Secure Cluster based VANET Modelling System with keyed Hash Message Authentication Code. International Journal of Emerging Technology in Computer Science & Electronics 23:135-140.

Poomagal, C.T., Sathish Kumar, G.A. ECC Based Lightweight Secure Message Conveyance Protocol for Satellite Communication in Internet of Vehicles (IoV). Wireless Pers Commun 113, 1359–1377 (2020). https://doi.org/10.1007/s11277-020-07285-3.

Rouissi N, Gharsellaoui H, Bouamama S (2019) Improvement of Watermarking-LEACH Algorithm Based on Trust for Wireless Sensor Networks. Proce-

dia Computer Science 159:803-813. doi: 10.1016/j.procs.2019.09.239.

Ramesh, S., Yaashuwanth, C. Enhanced approach using trust based decision making for secured wireless streaming video sensor networks. Multimed Tools Appl 79, 10157–10176 (2020). https://doi.org/10.1007/s11042-019-7585-5.

Singh, S. K., Bose, R., & Joshi, A. (2018). Energy theft detection in advanced metering infrastructure. 2018 IEEE 4th World Forum on Internet of Things (WF-IoT). doi:10.1109/wf-iot.2018.8355148.

Shen, J., Wang, C., Castiglione, A., Liu, D., & Esposito, C. (2017). Trustworthiness Evaluation-based Routing Protocol for Incompletely Predictable Vehicular Ad hoc Networks. IEEE Transactions on Big Data, 1–1. doi:10.1109/tbdata.2017.2710347.

Selvi, M., Thangaramya, K., Ganapathy, S. et al. An Energy Aware Trust Based Secure Routing Algorithm for Effective Communication in Wireless Sensor Networks. Wireless Pers Commun 105, 1475–1490 (2019). https://doi.org/10.1007/s11277-019-06155-x.

Singh, O., Singh, J., & Singh, R. (2017). Multi-level trust based intelligence intrusion detection system to detect the malicious nodes using elliptic curve cryptography in MANET. Cluster Computing, 21(1), 51–63. doi:10.1007/s10586-017-0927-z

Sultana, J., & Ahmed, T. (2017). Securing AOMDV protocol in mobile adhoc network with elliptic curve cryptography. 2017 International Conference on Electrical, Computer and Communication Engineering (ECCE). doi:10.1109/ecace.2017.7912964

Tan, S., Li, X., & Dong, Q. (2016). A Trust Management System for Securing Data Plane of Ad-Hoc Networks. IEEE Transactions on Vehicular Technology, 65(9), 7579–7592. doi:10.1109/tvt.2015.2495325.

Yu, X., Li, F., Li, T. et al. Trust-based secure directed diffusion routing protocol in WSN. J Ambient Intell Human Comput (2020). https://doi.org/10.1007/s12652-020-02638-z.