IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 28 June 2022, accepted 20 July 2022, date of publication 1 August 2022, date of current version 17 August 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3195240

RESEARCH ARTICLE

A Concealed Based Approach for Secure Transmission in Advanced Metering Infrastructure

OTISITSWE KEBOTOGETSE, (Member, IEEE), RAVI SAMIKANNU, (Senior Member, IEEE), AND ABID YAHYA, (Senior Member, IEEE)

Department of Electrical, Computer and Telecommunications Engineering, Botswana International University of Science and Technology, Palapye, Botswana

Corresponding author: Otisitswe Kebotogetse (ko19100017@studentmail.biust.ac.bw)

This work was supported by the Botswana International University of Science and Technology under Grant S00172.

ABSTRACT The smart grid has an important subsystem known as the Advanced Metering Infrastructure (AMI), responsible for measuring customer consumption of electricity. The AMI subsystem has smart meters as one of the components and they play a vital role in enabling communication between the utility provider and consumers. Smart meters can report real-time electricity consumption readings of the consumer to the utility. Securing this communication link from attacks remain very important for the secure transmission of readings. Different methods or approaches have been developed, and most works have high computational overheads. This paper proposes a lightweight Concealed Based Security Scheme (CBSS) for secure transmission within the AMI, providing authentication, and reducing the computational overheads and energy consumption during transmission. The CBSS method is compared with the AMI Data Communication Scheme (ADCS) which does not have authentication process. The network is built in the Network Simulator 2 environment, showing the communication between the nodes. Further security is provided using a simple encryption/decryption method of 2 random numbers. The contribution of this paper is the proposed lightweight method for the AMI that authenticates the transfer of data between smart meters and other components of the AMI system. The paper also contains a simulation evaluation for the chosen design parameters of the resemblance of AMI network. The simulations show an improvement of 5% in delivery ratio, 3% throughput and 4% in energy consumed when adding security to the network.

INDEX TERMS Advanced metering infrastructure (AMI), decryption, encryption, network simulator 2 (NS2), smart grid, smart meter.

I. INTRODUCTION

The Smart Grid (SG) is an example of Cyber Physical Systems (CPS) and functions as Internet of Things (IoT) at substation level for example smart connected homes [1], [2]. Internet of Things is described as connecting intelligent objects in a network to perform everyday tasks. Human Beings and other sensor devices interact or communicate with these objects through the internet. The smart grid consists of digital and electrical technologies communicating and passing information from one device to another [3]. Advanced Metering Infrastructure (AMI) is one component that makes up the smart grid. The AMI's major role is to simplify meter readings from smart meters to the control center and the users. The bidirectional communication capability makes the AMI perform the role efficiently [4]. The introduction of the smart grid to the electrical industry has brought along new challenges. One of the challenges is security. This is very important for secure communication and detecting any malicious activities that might occur during transmission. In AMI, the smart meters are placed in consumer homes and exposed to being tempered. The

The associate editor coordinating the review of this manuscript and approving it for publication was Bin Zhou.

smart meter continues to require suitable methods of security. The location of these smart meters and the network in which these meters communicate, increase the chance of attack or vulnerability to attacks of the smart meter [5]. The most famous reasons for securing smart meter and the communication network involved are:

If data is altered, the predictions at the utility provider will be wrong [6].

If data is altered, it can lead to financial loss for the utility provider.

Disturbance of communication network due to some attacks may cause power cuts.

Attacks on service delivery may lead to power theft [7].

The encryption of data readings during transmission and decryption at the receiver side remains the highly used method of security in AMI [8]. Encryption hides data packets before the packets are sent into the network by using any format that is not understandable to unauthorized access [9]. Decryption discloses the cipher text to the original data packets before the hiding process. The authorized receiving node does decryption. Key-based cryptography is being adopted to secure communication between smart meters and other devices in the AMI architecture [10]. The management and secure generation of these keys remains an open challenge. This paper proposes a lightweight concealing-based AMI validation and secure transmission method that minimizes computational costs. The method is suitable for smart meters. The paper discusses the background and related work in section 2, the methodology of the proposed work in section 3, simulation results in section 4 and the conclusion in section 5.

II. BACKGROUND AND RELATED WORK

A. SMART GRID

The smart grid or power grid has many components working in different phases. The power generation phase and components are working there, there is the distribution, consumption and billing phases all have different components working in them, too [11].

B. AMI

The AMI is situated between the consumer and utility provider [12]. The AMI routes data of consumers' consumption through a wired or wireless network to the utility provider and gives the consumer billing data. The system works bi-directional communication to pass data between consumers and utility providers [13]. The nodes found in the AMI system communicate in three schemes multicast, broadcast and unicast [10]. The AMI has brought about different improvements to the original metering system. It has brought about flexibility, thus accommodating new users daily. Security and reliability have been improved as the system can adapt to changing technologies. The AMI also provides better accuracy in the billing information. The Smart meter is one of the components of the AMI system and it is responsible for generating consumption readings. It has brought about intelligence to the original energy meters [14].

C. SMART METER

The smart meter is an electronic device used to measure and record customer's electricity consumption and send the information to the utility provider for billing information. Smart metering is seen as a driver for energy efficiency and adoption of digitization [15]. Some countries adopted the smart meter technology and legally binds consumers who use more than 6000 kilowatt-hours (kWh), for example Germany [16]. Smart electricity meters use digital rather than electromechanical technology [17]. The major difference between the smart meter and modern measuring or metering equipment is that they take control over functions [18].

The smart meter is a device that was developed to act as a gateway for the smart grid to household devices [19]. It records the power consumption at the consumer location and periodically directs it to the utility provider. Smart meter also performs routing functions during communication in the Meter Data Management System. It routes packets to closer or neighboring meters until the packets reach their destination.

Communication technologies are used in smart metering network like the one shown in figure 1. Some commonly used technologies are Zigbee, Wifi and Bluetooth. In [21] researchers developed a multi-communication based AMI device specific for smart metering. According to the work, smart meters can use cellular and low power technologies to communicate with the utility server.

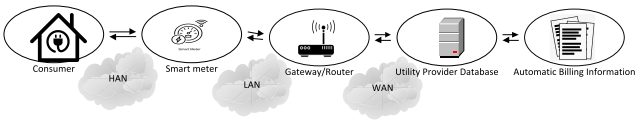

FIGURE 1. Basic AMI system structure showing smart metering process [20].

D. RELATED WORK

In [22] a system based on Diffie-Hellman key exchange protocol was developed for authenticating smart grid nodes. The system had high computational overheads and was based on traditional Public key. [23] Proposed key management schemes focused on unicast and multicast communication in the smart grid. The scheme suffered from the inherent problem of key escrow. In [24] a spanning tree key management method was developed for rekeying. The method was vulnerable to attackers since the rekeying process was done on a global key. [25] Proposed a method that used a gateway and sensor nodes. The method was based on key agreement as it used public-key cryptography. The nodes were grouped into Clusters and keys were shared in these clusters. The method reduced computational overheads but compromised security as many nodes are affected if the secret key of the cluster is known.

TABLE 1. Comparison of security and data management solutions.

Reference	Description	Strength	Weakness
[26]	An energy efficient cross layer sensing clustering method based on intelligent fog computing	The overheads are improved and lifetime of network is increased	The method is not secure against malicious attacks
[27]	Trust Management-Based Secure Routing Scheme for WSN	The scheme is energy efficient and data delivery ratio is increased	The scheme has route request responses that lead to more or increased overheads
[28]	A dynamic energy management system using smart metering	The method is energy efficient and reduces costs on the demand side	In this method security of AMI is compromised.
[29]	A source anonymity-based lightweight secure AODV protocol for fog based MANET	The protocol reduces energy consumption and the network's throughput is made better.	The method does not consider multi factors when routing is done. Latency is also compromised in this method when dealing with large scale nodes.
[30]	Design Implementation and Deployment of an IoT Based Smart Energy Management System	The method provides a solution to manage energy consumption at the consumer's side	Data security is ignored in the method
[31]	Data collection from WSNs to the cloud based on mobile Fog elements	The method considers multi factors when routing data and reduces the consumption of energy	The method experiences more re-transmissions because of no network congestion measurement
[32]	Privacy Preserving KNN Classification Algorithm for Smart Grid	In this method, privacy is provided and the algorithm can be used for different IoT smart devices	The method can be attacked by Denial of Service attack when establishing a reconnection to the internet
[33]	Smart Grid Information Management System Relying on MAS Technology and Complex Scientific Management Thinking	The wok provided a management system that monitors, evaluates and maintains the status of the smart grid.	The work ignores security and has complex computations that is not suitable for smart meters
[34]	Anonymous and Efficient Message Authentication Scheme for Smart Grid	The method provided authentication and addressed the drawbacks in Li's authentication scheme	The communication costs are ignored
Proposed Scheme	A Concealed Based Security Scheme for Advanced Metering Infrastructure	The Scheme reduced energy consumed by nodes and provides authentication on the AMI network	The method only consider security on the AMI communication nodes.

III. METHODOLOGY

A. NETWORK MODEL

The AMI system's hierarchical linkages are made up of sensors $S = s_1 \ldots, s_n$, base stations B_S, web servers W_S, application providers A_P, Internet portals I_P, and users connected to smart metres S_M.

The smart meter's sensors measure consumption data and send it to the B_S through a safe channel. The data is then distributed or shared with the relevant users which are customers. Multi-hop communication has been adopted between the sensors and the users. An Internet gateway connects the B_S and the W_S in the hierarchical structure as shown in figure 2. The sensors provide the data for meter readings and utility provider P_U provides the bill details, which are transferred to the W_S and then to the user.

B. NETWORK INFRASTRUCTURE

The W_S acts as an interface between the B_S, the user and the P_U. Users use the I_P as an interface to communicate with the S_M through its W_S infrastructure. Data transfer takes place from time to time between the W_S and the sensors.

The sensors detect data and communicate it to the B_S utilising multi-hop communications from time to time throughout the detection period. The data is sent from the B_S

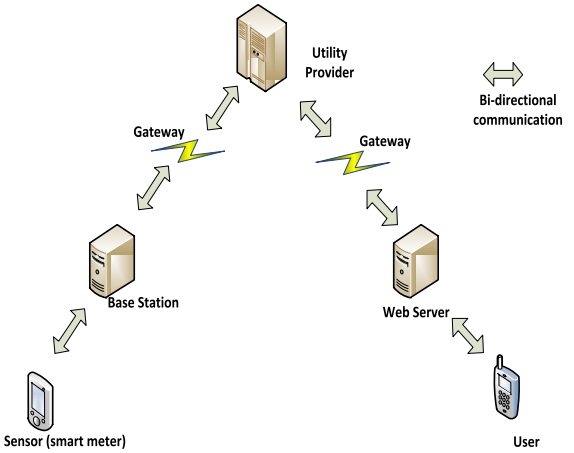

FIGURE 2. Network model for AMI infrastructure.

to the W_S via an associated gate-way G_W, which then stores it at the P_U, each user is connected to one or more sensors because one user can have more than one home, the sensors are managed by the connection at the provider's web server. The user device connects to the W_S to retrieve sensitive data from the linked sensor during the data retrieval period. There is communication between the sensor and the user through the internet portal.

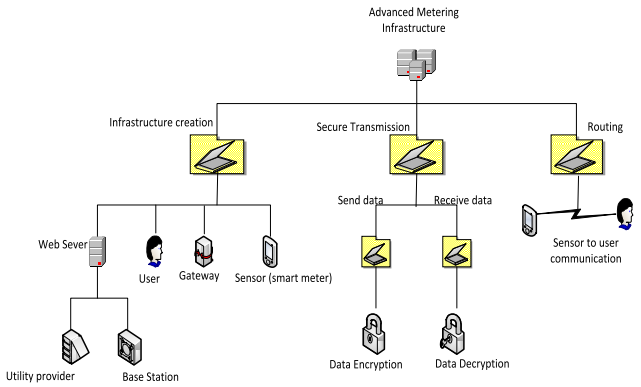

FIGURE 3. Architectural summary of the proposed work.

C. SECURITY WADER EMPOWERED

The secure minimum weight shared key creation and data protection will be invoked when the connection configuration has been formatted. The sensor sends a trajectory request to the web server authentication server during the security boot procedure. The web server receives the trajectory request and generates a start-up table S_{UT} and a communication sub-table C_{ST}. R is the communication range of trajectory information. The server starts with two tables S_{UV} and C_{SV}. Data is stored in these tables and certain variables are represented in matrices. For each meter, the bit vectors are then classified into several columns to store the data, also meters are periodically reassigned with security measures to improve security communications.

Check data length

$$S_{UTi} = (0, R) \tag{1}$$

$$C_{STi} = (0, R) \tag{2}$$

Both tables are generated randomly independent of the device identities and are organized in the matrix structure in terms of binary bits as given in Table 2. In matrix format, data is represented as binary. Each bit is XORED (using exclusive or function) with the corresponding array node.

TABLE 2. Example of the check data length process.

S_{UTi}	C_{STi}
10000010	11001000
00111101	01111011
00110000	01011000
01110001	00010011
11000101	11001000
11110001	00111010
11000110	01010110
10001011	00111011

The table is encrypted using the keys generated from the remainder statement. Here N_{ID} is the node ID and T is the time of communication. As the keys are shared on the network, its processing time increases. To evade this, each meter generates the S_K and C_K keys from the built-in main key with the support of credential authority C_{RA}. Bits of data associated with S_{UT} and C_{ST} will be XORed. S_{UT} and C_{ST} are further encrypted by the S_K and C_K keys using the concealing method.

$$S_K = K \; xor \; N_{ID} \tag{3}$$

$$C_K = K \; xor \; T \tag{4}$$

Here, S_K is the S_{UT} key and C_K is the C_{ST} key. The first key S_K was generated using the xor function of the primary key and the node identifier. The second key C_K was generated using the xor function of the main key and the current time C_T in the communication session. Once S_K and C_K are generated, S_{UT} and C_{ST} are encrypted using the keys, correspondingly. At the receiver end, xor is extracted from S_K and C_K messages using the reverse process of operation as C_{STEi}, S_{UTEi}.

$$S_{UTEi} = S_{Vi} \; xor \; S_K \tag{5}$$

$$C_{STEi} = C_{Vi} \; xor \; C_K \tag{6}$$

The meter reading is xor with the tables generated continuously, and these tables are encrypted using the xor function.

D. KEY GENERATION DEVELOPMENT

The process is further advanced using elliptical curve cryptography E_{CC} and fully hashing method. The authentication server acts as credential authority C_{RA} between the sensor and the user. During the initialization process, the C_{RA} generator selects curve parameters

C_P such as curve points P_T, prime numerals P_N, curve factor C_F, and defined prime pitch P_P. The bilinear map is

created when we first start the security process, in which some basic things are created. That is, some prime numbers P_N, some rotation groups are formed in the order of P_N as follows, G_i, G_j, G_k. Here, A number divisible by the same number and only one is called a prime number.

$$choose\ i\ from\ 0\ to\ 998 \tag{7}$$
$$choose\ j\ from\ 0\ to\ 999 \tag{8}$$
$$choose\ k\ from\ 0\ to\ 1000 \tag{9}$$
$$If\ (i \neq j \text{ and } j \neq k \text{ and } i \neq k) \tag{10}$$
$$If\ \ e\ (j, i+k) = e\ (i+k, j)\ \ and\ e(i+k, j) \tag{11}$$

Rotation groups are called the subgroup of E_{CC} that defined a field. It supports to regulate the magnitude of the number in calculation. Then update groups as G_i, G_j, G_k. After adding numbers to that group, the values within that particular number are taken as a and b and p is selected and added to the final group. With this, the map e and its generators a and b are created. Here the computations of $(f-g)(f+g)$ returns the e map function values. The prime number is calculated as follows, of which, i is taken as the number 2 also, the value of i is less than a.

Similarly, the values of i will be constantly updated. If the value of a mod i is 1 then it is called prime. After that, the selected P_N numbers will be added to the table called Z_P. When using random numbers R, we select a number from 0 to Z_P and use it.

$$R = OS2IP(SHA1(Z_P(R))) \tag{12}$$

These Z_P values help create random numbers and multi calculations needed to increase security on the network. And with the help of these numbers one-way hash H_1 code is generated. At the beginning of the network, all meters, B_S, *and* G_W in that region communicate with the credential authority and are authenticated. Each time the sensors in the meters send a control message before sending the data. The authorization of the meter is then validated and the contacts are processed. Each time the meters make contact, the meter's authentication and key transmission functions are called. The sensors send information about the meter they have sensed to the credential authority. Once the server recognizes the meter, a unique U_K and common key P_K is generated for the sensor. The curve points are selected according to the inputs I_P such as (P_N, P_T, P_F, x, y). A U_K and the P_K are generated after selecting a R number from it. Here, x and y are the curve constant values. P_F is the prime pitches and is the P_T point of elliptic curve. These values are used to generate the pseudo arbitrary numeral values and multi factor calculations.

$$X = (S_{ID}, R) \tag{13}$$
$$U_K = (D_P, X) \tag{14}$$
$$P_K = (R, U_K) \tag{15}$$

Later meter public key P_K is generated according to curve P_T. Here we use D_P from the basic parameter of the elliptic curve.

The generated key K pair is sent to the meter channel and the same process is repeated for all devices.

$$K = (U_K, M) \rightarrow M_{ID} \tag{16}$$

If it is not unique, the credential authority will need to re-create the identity M_{ID} approximately for the specific meter. Once the key transfer process between the sensor and the C_{RA} is complete, mutual recognition will be created between the final devices. Also, public key is used at data transmission and private key.

E. NETWORK FORWARDER SELECTION AND ALGORITHM FLOW

During the initial operation of mutual recognition between M and G_W, the prime number R is selected from the curve generated. The random number is multiplied by the generator point and R is generated to identify the time- cast T_C. Here C_T is the current time.

$$T_C = C_T \tag{17}$$
$$G_K = (R, S_P, T_{SM})(G_{WR}, G_P) \tag{18}$$

Here G_K is the gateway private key. Each M generates a random number. We call this $R \rightarrow M_R$. It will be extracted from the created Z_P numbers. It is calculated as N, here $N = (I_P M_R)$, I_P is the used input parameters.

$$G_{Wr} = OS2IP(SHA1(N)) \tag{19}$$
$$G_{WR} = I_P G_{Wr} \tag{20}$$
$$G_P = P_K(M_R) \tag{21}$$
$$S_P = P_K(G_P) \tag{22}$$

Here, G_P is the gateway public key. G_{WR} this is the random number selected for the gateway. Then we calculate the two hash values f and g as below. S_P is the smart meter public key.

$$f = H_1(R, S_P, G_{WR}, G_P, T_{CS,} T_{GW,}) \tag{23}$$
$$g = H_1\left(G_{WR}, R, S_P, G_P, T_{GW,}, T_{CS}\right) \tag{24}$$

Every time there is a connection in the network, the sensor's neighbor gateway checks the time of the message sent by the sensor along with time $T_{CS,}$ and checks the random number in the group we created on the bilinear map. This number will be selected as a random number from new $G_{WR} \in S_P$. And calculates the corresponding R according to the elliptic curve point multiplication technique. The time at which this process is completed is then denoted as $T_{GW,}$ as gateway The derived secure validation code is compared to the reverse authentication code generated. The connection will be maintained until the last device is successfully verified if a match is found. The shared key derivative function is enabled after successful verification, with I_{SM}, T_{CS}, and T_{GW} serving as the session's key generating entries.

The secure authentication meter is now computed as the second level hashed value, such as H_2 $(I_{SM}, T_{CS}, f_{SM}R)$ and the hashed value is transmitted to finish the mutual validation procedure. The device re-generates the secure code

Algorithm 1 Concealed Based Security Scheme (CBSS) for AMI Communication

1. *Chosoe* $R = OS2IP(SHA1(Z_P(R)))$
2. *Update Current Time* $C_{Tas}T_C$
3. *Chosen Inputs to Finalize the Key*(P_N, P_T, P_F, x, y)
4. *CreateT*$_C$ *for Sensor* T_{CS} *and Gatewayas* T_{GW}
5. *Create a Gateway Random Numeral* $G_{WR} \in Z_P$
6. *Generate Unique and public keys as below*
7. $X = (S_{ID}, R)$
8. $U_K = (D_P, X)$
9. *Meter Public Key* $P_K = (R, U_K)$
10. *Computed Meter private Key* $K = (U_K, M) \rightarrow M_{ID}$
11. *Gateway Private Key Created* $G_K = (R, S_P, T_{SM})(G_{WR}, G_P)$
12. *Gateway Random Number* $G_{Wr} = OS2IP(SHA1(N))$
13. $G_{WR} = I_P G_{Wr}$
14. *Gateway Public Key* $G_P = P_K(M_R)$
15. *Meter Public Key* $S_P = P_K(G_P)$
16. *Hash Value Computed Below*
17. $f = H_1(R, S_P, G_{WR}, G_P, T_{CS}, T_{GW},)$
18. $g = H_1(G_{WR}, R, S_P, G_P, T_{GW},, T_{CS})$
19. *Additional New Values Computed*
20. $S_{GW} = (g + G_{WR})f\%v$
21. $I_{GW} = S_{GW}(R + fS_P)$
22. *Secure validation code created* $H_2(I_{GW}, T_C, f_{GW}G_{WR})$
23. *Secure Meter selected* $H_2(I_{SM}, T_{CS}, f_{SM}R)$
24. *Secure Receiver Slected* $H_2(I_{GW}, T_{GW}, RS_P)$
25. *Reverse Validation Code* I_{GW}, T_{CS}, G_{WR}*toFinalize the path*

authentication meter as a second level hashed value of the H_2 (I_{GW}, T_{GW}, RS_P) at the receiver end.

The secure meter is now calculated as I_{SM} secondary hash value H_2, T_{CS}, $f_{SM}R$, the hash value is provided to complete the mutual secure validation procedure. After receiving the data, the device reproduces the validation code to secure the meter.

The transmitter device is considered to have been successfully checked if the generated code matches the received code. Using the key derivative function, shared keys are now generated as inputs with I_{GW}, T_{SM}, and time. After that compute $(R + f^2)$ % v and $S_{GW}(G_{WR} + gG_P)$ are the new values for meter and additional value of I_{GW}, respectively. The secondary hash value H_2 of S_P is derived as the reverse authentication code (I_{GW}, T_C, G_{WR}).

$$S_{GW} = (g + G_{WR})f\%v \tag{25}$$

$$I_{GW} = S_{GW}(R + fS_P) \tag{26}$$

Both R and T_C are sent to the final device to establish the mutual validation process. The device receives and verifies T_C and R. Upon successful verification, the device randomly selects its number G_{WR} from the P_N curve and multiplies it with the generator point.

It is marked as G_{WR} and the T_{GW} is estimated as the current time-stamp. From the public-private key pairs (f_{SM}, G_{WR}), S_P and G_{WR} is identified for the end devices. Now, using the R, G_{WR}, S_P, G_P, T_{CS}, and T_{GW} as inputs, the exchange parameters f and g are calculated using the single-way hash function.

Now $S_{GW}, G_{WR} + gf_{GW}$ is calculated as% v, where v is the curve point, S_{GW} and I_{GW} which are the cross-parameters of the two end devices. The final validation code is generated as a H_2 $(I_{GW}, T_C, f_{GW}G_{WR})$. The value generated to verify the correctness of the security system is sent to the other end device. The device confirms the ownership of T_{GW} and G_{WR}. If the verification is successful, the reverse transmission parameters are calculated using the hash function for f and g inputs R, G_{WR}, S_P, G_P, T_{CS} and T_{GW}.

Now another refine estimation S_{GW} and I_{GW} are calculated as follows, $R + ff_{SM}\%v$ and $S_{MR}(G_{WR} + gS_P))$ respectively. The reverse validation code $I_{GW}, T_{CS,}G_{WR}$ is calculated as the secondary hash value of G_P.

T_{GW} entries. The shared key executes encryption and decryption during data transmission operations.

TABLE 3. Simulation parameters on network simulator 2.

Parameters	Values
Simulation Time	Variable (seconds)
Field Size	500 x 500 m^2
Channel	Wireless
Antenna	Omni Antenna
MAC type	Mac/802.11
Routing Protocol	Advanced On Demand Vector (AODV)
Number of Nodes	101

IV. PROTOTYPE DEVELOPMENT

The nodes involved are BS (Base Station), WS (Web Server), GW (Gate Way), UP (Utility Provider), Users (Customers) and Sensors (Smart meters).

At the beginning of the communication, every node identifies its neighbours. The nodes hello messages and acknowledge each other and form a connection. The main communication is between the sensors and the users. The other nodes are just intermediate devices. The sensor measures consumption readings and forwards them to the BS, then the BS forwards to the GW, and finally, the readings reach the Utility provider. The billings are created here, sent to the GW, and then to the User. The user can see the readings sent from the sensor and the billing information. The communication that takes place between the nodes is bi-directional. Sending some packets in the network requires an acknowledgment from the receiver.

The security aspect of the communication is also addressed. The sensor does the encryption and the user does the decryption. At the sensor, the readings are distorted into some form of text called cipher text. The text does not make sense to anyone who comes across it unless you have the decryption method to turn back the cipher text to plain text. In the communication network, the user is the only node with the decryption method. The decryption method only sends the cipher text to the specific user. This is done by including the destination identity in the transmitted packet.

The chosen scenario in the NS2 environment shown in Table 3 gives the figures 4-7. A network area of 500 by

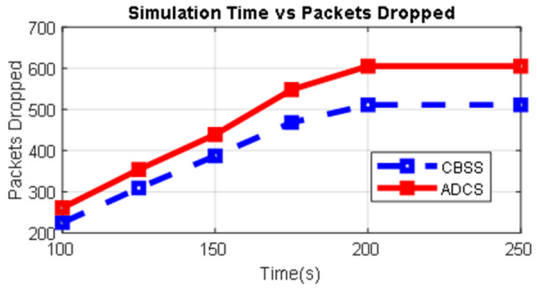

FIGURE 4. Impact of varying simulation time on: Packets dropped during transmission of data.

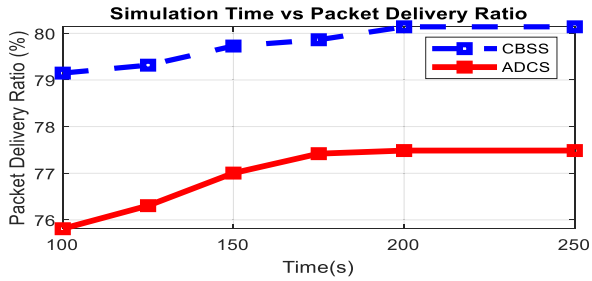

FIGURE 5. Impact of varying simulation time on packets delivery ratio during transmission of data.

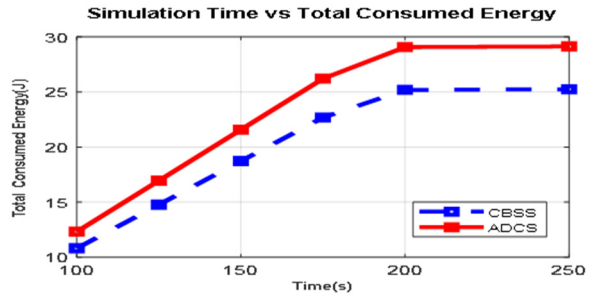

FIGURE 6. Impact of varying simulation time on: Total consumed energy during data transfer.

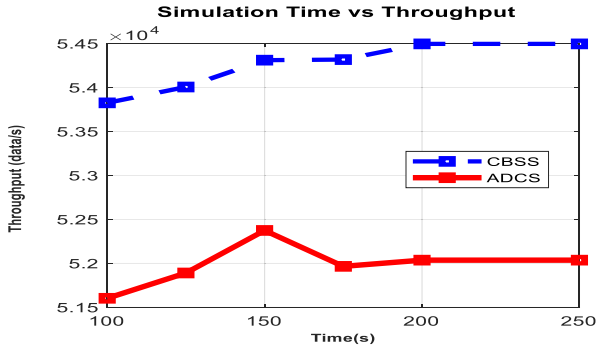

FIGURE 7. Impact of varying simulation time on throughput during data transfer.

500 was chosen and 101 nodes were randomly placed within the network area. The parameters are selected to resemble a real Advanced Metering Infrastructure environment. The paper evaluated the performance of AMI when having security and without security. After simulations, certain parameters were measured and the graphs below show the results from the simulations. The network area is determined by the number of nodes in the network. The nodes should not overlap in the network. Omni Antenna is the popular antenna used for nodes in the network simulator 2 environment and the Advanced On Demand Vector routing protocol transports data faster than other routing protocols.

The metrics of interest are the packets dropped, packet delivery ratio, total energy consumed, and throughput. These are the parameters measured when comparing the two methods of having security and not having security in AMI communication.

A. PACKETS DROPPED

These are data packets lost during transmission and are not received by receiver nodes. The sender's packets are originally sent but do not reach the destination nodes [35]. Packet dropping increases data errors during communication. The main cause of packet dropping is network congestion. The throughput of a given sender is affected by packet drop. When the packet dropping is very high in the network, important data packets do not reach the intended destination. This is a sign of a bad communication network. It can be expressed by:

Packets dropped = Total Packets sent by all sender nodes – Total packets received by all receiver nodes

B. PACKET DELIVERY RATIO

This ratio of packets received by the receiver nodes and packets sent by the sender nodes [36].

The performance of a network is said to be higher when the packet delivery ratio is high. It can be expressed by:

Packet delivery ratio = Total Packets received by all destination nodes/Total Packets sent by all sender nodes

C. TOTAL ENERGY CONSUMED

combines energy used during transmission, computation, and reception [37]. It has been known that energy is consumed more during transmission and reception. The computation process consumes less energy [38]. It can be expressed by:

Total energy consumed = Transmission energy + Computation energy + reception energy

D. THROUGHPUT

Throughput is the amount of data packets successfully reaching the receiver from the sender at a given period. It is usually measured in bytes/second. Low bandwidth, low energy, unreliable node communication, and topology change impact throughput. It can be expressed by:

Throughput = File size / Transmission time

V. RESULTS AND DISCUSSION

Figure 4 shows that the number of packets dropped increases with simulation time. The CBSS during data transmission provides better packet dropping than when there is ADCS.

The more secure the transmission, the lesser packets are being dropped. The packet dropping shows a huge difference between the two methods from 200 to 250 seconds of simulation time. At these times, the difference is constant. From the simulation results at 200 seconds, packets sent were 2573 for both methods. ADCS received 1968 packets, thus dropping 605 packets (24%). CBSS in the network, 2071 packets were received and 502 packets dropped (19% packets dropped). This is due to the difference in security between the two networks. The attacks affect the ADCS method due to a lack of authentication leading to packets that do not reach the destination nodes, and more congestion in the network.

Figure 5 shows the packet delivery ratio increase when simulation time increases. When the transmission in AMI is more secured, the delivery ratio is increased. The delivery ratio follows similar conditions as the graph in Figure 4. The simulation at 200 seconds will also be used as an example here. 2573 packets were sent in the network and simulation was made using the ADCS method, 1968 were received. Similar conditions were made using the CBSS method and 2071 packets were received. The delivery ratio is 76% without security and 81% with security. The delivery ratio of packets transmitted in the ADCS is lower than those transmitted in CBSS. The more secure the transmission, the more the packet delivery ratio. Security prevents attacks from affecting packets during transmission. As many packets reach their destination nodes, reducing malicious activities increases the delivery ratio.

Fig. 6 shows that energy is consumed more when there is less security and less when the network is made more secure. At 200 seconds, the simulation of ADCS consumed 29% of the energy given, and the simulation of CBSS consumed 25% of the energy given. The packets are exposed to replay attacks during transmission in the two methods, leading to more energy consumption in the ADCS method than in the CBSS method. Security reduces forged data traffic in the AMI network, reducing the energy consumption of sensor nodes.

Figure 7 shows that the throughput in CBSS is better than ADCS. The percentage difference in the throughput between the two graphs is around 3%. The difference is caused by many factors like reliability between communication nodes. From Figure 4, we already indicated that network congestion affects simulation in ADCS more, so bandwidth becomes limited or low when there is more congestion, causing the throughput to be reduced. Throughput is also affected by low energy. When more energy is consumed, as shown in Figure 6, the remaining energy becomes less, causing the throughput to be reduced.

VI. CONCLUSION

The Concealed Based Security Scheme (CBSS) method for secure transmission is the best method when reducing computational costs and energy consumption in AMI. The results show the difference between a network with AMI Data Communication Scheme (ADCS) and a network with CBSS. The graphs show an improvement in energy consumed of 4%, 3% throughput, and 5% delivery ratio since the security provided in the two methods is different but at the same time uses simple cryptographic techniques to cater to low computational smart metering abilities. The CBSS method reduced the number of packets dropped, thus increasing the network's throughput. The energy consumption was also reduced, saving the power used up by the ADCS method. The idea was to provide security and, simultaneously, consider the low computational abilities of smart meters. Most security methods ignore the ability of smart meters not to compute difficult computations and only focus on security being provided, in return giving slow processing times. The CBSS method considers faster processing time, thus the reason for having small computations when providing security. The process can be improved in the future by using an elliptic curve and a fully hashing method for key generation to make the system more secure. Different types of attacks can be introduced to the network and the methods tested against these attacks as one of the improvements to be considered in the future.

REFERENCES

[1] M. Nabeel, X. Ding, S.-H. Seo, and E. Bertino, "Scalable end-to-end security for advanced metering infrastructures," *Inf. Syst.*, vol. 53, pp. 213–223, Oct. 2015, doi: 10.1016/j.is.2015.01.004.

[2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, Oct. 2015, doi: 10.1109/COMST.2015.2444095.

[3] J. S. Hong and M. Kim, "Game-theory-based approach for energy routing in a smart grid network," *J. Comput. Netw. Commun.*, vol. 2016, pp. 1–8, Jan. 2016, doi: 10.1155/2016/4761720.

[4] S. P. Kumar, H. T. Ansari, and V. Saminadan, "Smart grid communication architecture modeling for heterogeneous network based advanced metering infrastructure," *Int. J. Electron. Commun. Eng.*, vol. 11, no. 4, pp. 405–410, 2017. [Online]. Available: https://core.ac.uk/download/pdf/144880223.pdf

[5] A. M. Khattak, S. I. Khanji, and W. A. Khan, "Smart meter security: Vulnerabilities, threat impacts, and countermeasures," *Adv. Intell. Syst. Comput.*, vol. 935, pp. 554–562, Jul. 2019, doi: 10.1007/978-3-030-19063-7_44.

[6] J. Peppanen, X. Zhang, S. Grijalva, and M. J. Reno, "Handling bad or missing smart meter data through advanced data imputation," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Sep. 2016, pp. 1–5, doi: 10.1109/ISGT.2016.7781213.

[7] R. Czechowski and A. M. Kosek, "The most frequent energy theft techniques and hazards in present power energy consumption," in *Proc. Joint Workshop Cyber Phys. Secur. Resilience Smart Grids (CPSR-SG)*, Apr. 2016, pp. 1–7, doi: 10.1109/CPSRSG.2016.7684098.

[8] M. M. Hasan and H. T. Mouftah, "Encryption as a service for smart grid advanced metering infrastructure," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2015, pp. 216–221, doi: 10.1109/ISCC.2015.7405519.

[9] G. C. Kessler. (1998). *An Overview of Cryptography Updated Version*. [Online]. Available: https://www.garykessler.net/library/crypto.html

[10] O. Kebotogetse, R. Samikannu, and A. Yahya, "Review of key management techniques for advanced metering infrastructure," *Int. J. Distrib. Sensor Netw.*, vol. 17, no. 8, Aug. 2021, Art. no. 155014772110415, doi: 10.1177/15501477211041541.

[11] M. E. El-hawary, "The smart grid—State-of-the-art and future trends," *Electr. Power Compon. Syst.*, vol. 42, nos. 3–4, pp. 239–250, Mar. 2014, doi: 10.1080/15325008.2013.868558.

[12] J. F. Martins, A. G. Pronto, V. Delgado-Gomes, and M. Sanduleac, "Smart meters and advanced metering infrastructure," *Pathways Smarter Power Syst.*, vol. 2017, pp. 89–114, Oct. 2019, doi: 10.1016/b978-0-08-102592-5.00004-1.

[13] T. Rosfjord, P. Manager, A. Chen, J. Mulugeta, and T. Bhatia, "Advanced microturbine systems," Final Rep. DOE/CH/11060-1, 2007, p. 155.

[14] H. Road and T. Benjamin, "AMI meter electromagnetic field survey," Oct. 2011, pp. 1–62.

[15] T. Knayer and N. Kryvinska, "An analysis of smart meter technologies for efficient energy management in households and organizations," *Energy Rep.*, vol. 8, pp. 4022–4040, Nov. 2022, doi: 10.1016/j.egyr.2022.03.041.

[16] F. Tounquet and C. Alaton, "European commission," 2019, doi: 10.2833/492070.

[17] P. Umang and M. Mitul, "A review on smart meter system," *Int. J. Innov. Res. Elect., Electron., Instrum. Control Eng.*, vol. 3, no. 12, pp. 70–73, Dec. 2015, doi: 10.17148/ijireeice.2015.31215.

[18] M. S. Javadi, A. E. Nezhad, M. Gough, M. Lotfi, A. Anvari-Moghaddam, P. H. J. Nardelli, S. Sahoo, and J. P. S. Catalão, "Conditional value-at-risk model for smart home energy management systems," *e-Prime*, Oct. 2021, Art. no. 100006, doi: 10.1016/j.prime.2021.100006.

[19] K. Förderer, M. Lösch, R. Növer, M. Ronczka, and H. Schmeck, "Smart meter gateways: Options for a BSI-compliant integration of energy management systems," *Appl. Sci.*, vol. 9, no. 8, pp. 1–19, 2019, doi: 10.3390/app9081634.

[20] A. Hassan, H. N. Afrouzi, C. H. Siang, J. Ahmed, K. Mehranzamir, and C.-L. Wooi, "A survey and bibliometric analysis of different communication technologies available for smart meters," *Cleaner Eng. Technol.*, vol. 7, Apr. 2022, Art. no. 100424, doi: 10.1016/j.clet.2022.100424.

[21] S. Jain, M. Pradish, A. Paventhan, M. Saravanan, and A. Das, "Smart energy metering using LPWAN IoT technology," in *Proc. ISGW*, 2018, pp. 19–28.

[22] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 675–685, Dec. 2011, doi: 10.1109/TSG.2011.2160661.

[23] B. Alohali, K. Kifayat, Q. Shi, and W. Hurst, "A survey on cryptography key management schemes for smart grid," *J. Comput. Sci. Appl. Sci. Educ.*, vol. 3, no. 3A, pp. 27–39, 2015, doi: 10.12691/jcsa-3-3A-4.

[24] M. S. Yousefpoor and H. Barati, "Dynamic key management algorithms in wireless sensor networks: A survey," *Comput. Commun.*, vol. 134, pp. 52–69, Jan. 2019, doi: 10.1016/j.comcom.2018.11.005.

[25] G. Mehmood, M. S. Khan, A. Waheed, M. Zareei, M. Fayaz, T. Sadad, N. Kama, and A. Azmi, "An efficient and secure session key management scheme in wireless sensor network," *Complexity*, vol. 2021, pp. 1–10, Jun. 2021, doi: 10.1155/2021/6577492.

[26] Z. Sun, L. Wei, C. Xu, T. Wang, Y. Nie, X. Xing, and J. Lu, "An energy-efficient cross-layer-sensing clustering method based on intelligent fog computing in WSNs," *IEEE Access*, vol. 7, pp. 144165–144177, 2019, doi: 10.1109/ACCESS.2019.2944858.

[27] W. Fang, W. Zhang, W. Chen, Y. Liu, and C. Tang, "TMSRS: Trust management-based secure routing scheme in industrial wireless sensor network with fog computing," *Wireless Netw.*, vol. 26, no. 5, pp. 3169–3182, Jul. 2020, doi: 10.1007/s11276-019-02129-w.

[28] N. T. Mbungu, R. C. Bansal, R. M. Naidoo, M. Bettayeb, M. W. Siti, and M. Bipath, "A dynamic energy management system using smart metering," *Appl. Energy*, vol. 280, Dec. 2020, Art. no. 115990, doi: 10.1016/j.apenergy.2020.115990.

[29] W. Fang, W. Zhang, J. Xiao, Y. Yang, and W. Chen, "A source anonymity-based lightweight secure AODV protocol for fog-based MANET," *Sensors*, vol. 17, no. 6, pp. 1–16, 2017, doi: 10.3390/s17061421.

[30] M. U. Saleem, M. R. Usman, and M. Shakir, "Design, implementation, and deployment of an IoT based smart energy management system," *IEEE Access*, vol. 9, pp. 59649–59664, 2021, doi: 10.1109/ACCESS.2021.3070960.

[31] T. Wang, J. Zeng, Y. Lai, Y. Cai, H. Tian, Y. Chen, and B. Wang, "Data collection from WSNs to the cloud based on mobile fog elements," *Future Gener. Comput. Syst.*, vol. 105, pp. 864–872, Apr. 2020, doi: 10.1016/j.future.2017.07.031.

[32] Z. Song, Y. Ren, and G. He, "Privacy-preserving KNN classification algorithm for smart grid," *Secur. Commun. Netw.*, vol. 2022, pp. 1–11, May 2022.

[33] J. Tong, "Smart grid information management system relying on MAS technology and complex scientific management thinking," *Discrete Dyn. Nature Soc.*, vol. 2022, p. 9, 2022, Art. no. 9443293. [Online]. Available: https://www.hindawi.com/journals/ddns/2022/9443293/, doi: 10.1155/2022/9443293.

[34] L. Wu, J. Wang, S. Zeadally, and D. He, "Anonymous and efficient message authentication scheme for smart grid," *Secur. Commun. Netw.*, vol. 2019, pp. 1–12, May 2019.

[35] M. F. Khan, E. A. Felemban, S. Qaisar, and S. Ali, "Performance analysis on packet delivery ratio and end-to-end delay of different network topologies in wireless sensor networks (WSNs)," in *Proc. IEEE 9th Int. Conf. Mobile Ad-hoc Sensor Netw.*, Dec. 2013, pp. 324–329, doi: 10.1109/MSN.2013.74.

[36] E. Fazeldehkordi, O. A. Akanbi, A. Study, and H. Attack, "A neoteric swarm intelligence stationed IOT–IWD algorithm for revolutionizing pharmaceutical industry leading to digital health," 2016.

[37] A. Saravanaselvan and B. Paramasivan, "Implementation of an efficient light weight security algorithm for energy-constrained wireless sensor nodes," *Circuits Syst.*, vol. 7, no. 9, pp. 2234–2241, 2016, doi: 10.4236/cs.2016.79194.

[38] M. A. Hamid and C. S. Hong, "Energy conserving security mechanisms for wireless sensor networks," *Ann. Telecommun. Annales des Télécommunications*, vol. 64, nos. 11–12, pp. 723–734, Dec. 2009, doi: 10.1007/s12243-009-0088-z.

OTISITSWE KEBOTOGETSE (Member, IEEE) received the M.Eng. degree in electronics, telecommunication and internet engineering from the University of Bradford, U.K. He is currently pursuing the Ph.D. degree in electrical, computer and telecommunications engineering with the Botswana International University of Science and Technology, Palapye, Botswana. He has a six year's experience working in the telecommunication industry in Botswana. He is also a Registered Member of Engineers Board of Botswana.

RAVI SAMIKANNU (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from Anna University, Chennai, India. He is currently working as an Associate Professor with the Electrical Engineering Department, Botswana International University of Science and Technology, Palapye, Botswana. He has a total teaching experience of 17 years at undergraduate and postgraduate levels. He has published 80 research articles in international journals. He has presented 50 papers in international and national conferences and has received the Best Paper Award two times for his presentation. He is as an Active Member in IDDS and participated in different rural community development projects.

ABID YAHYA (Senior Member, IEEE) received the bachelor's degree in electrical and electronic engineering majoring in telecommunication from the University of Engineering and Technology Peshawar, Pakistan, and the M.Sc. and Ph.D. degrees in wireless and mobile systems from Universiti Sains Malaysia, Malaysia. After bachelor's degree, he began his career on an engineering path, which is rare among other researcher executives. Currently, he is working at the Botswana International University of Science and Technology. He has many research publications to his credit in numerous reputable journals, conference articles, and book chapters. He has received several awards and grants from various funding agencies and supervised several master's and Ph.D. candidates.