RESEARCHERID
THOMSON REUTERS
[INIT: January 2017]
ISSN 2348 – 8034
Impact Factor- 4.022
GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

SECURINGDATAPACKETS IN SMART GRID WIRELESS COMMUNICATION USING ELLIPTIC CURVE CRYPTOGRAPHY

Neelima Sahu*
*M.E.CSE Asst. Prof, BrindavanCollege,Bengaluru

ABSTRACT

As we are moving from an age of manual operation to the automated age, there is a great demand of automatic completion of tasks in power sector also. In this direction smart grid can be considered as a milestone in power sector technology. Smart grids are deployed with wireless communication platform, which offers many advantages of flexibility, low cost, shared communication and mobility. But it also suffers from disadvantages of privacy andsecurity.The communication messages in smart grid contain information about customer usage, billing and other private customer data. This information must be securedCompared with traditional power networks, the characteristics of the smart grid power system make it easier to suffer from several types of security threats and attackssuchas impersonation eavesdropping and message modification.This paper tries to find an effective solution first by identifying the various malicious nodes with help of path tracing algorithm in the network of smart grid which uses AODV protocol for routing.Then data packets are encrypted using elliptic curve cryptographyalgorithm. The encrypted message is transferred in data packets along the randomly selected path.

I. INTRODUCTION

Over the last century, the current power grid has proved to be very efficient in delivering power for all our necessities. It is facing the problems of the limited delivery system, high cost of power outage and power quality interruption, inefficiency at managing peak load. To satisfy both the increasing demand for power and the need to reduce carbon dioxide emissions, there is a need an electric system that can handle these challenges in a sustainable, reliable and economic way. A smart grid is an enhancement of a common electrical network, which delivers electrical energy from suppliers to consumers. ASmart gridis a modernized electrical grid that uses analogue or digital information and communications technology to gather and act on information, such as information about the behaviours of suppliers and consumers, in an automated fashion to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity.Smart Grid facilitates efficient and reliable end-to-end intelligent two-way delivery system from source to sink through integration of renewable energy sources, smart transmission and distribution. At its core, a smart grid utilizes digital communications and control systems to monitor and control power flows, with the aim to make the power grid more resilient, efficient and cost effective. The basic objectives of smart grids are to enable informed participation by customers; accommodate all generations (solar, wind, etc.) and storage options; enable new products, services, and markets; provide the power quality needed for the range of needs in a 21st century economy; optimize asset utilization and operational efficiency; address disturbances through automated prevention, containment and restoration; and operate resiliently against all hazards.
There are several security techniques are available for dedicated information networks like third party authentication, intrusion detection system. But these cannot be applied to smart grids because of following drawbacks. [11] [12].

Low priced: For any user or supplier the first preference is the cost. The various reasons behind cost effectiveness are computational power, memory and storage. But Byzantine cryptographic algorithms drain all computation and storage of resource units. Third party applications, such a private key generator [13] may visibly increase the cost of the whole wireless system.

Low Bandwidth: The wireless channels in smart grids are designed to transmit short message which requires less bandwidth than traditional wired networks. Standard encrypted system typically adds 64 to 96 bits to every message which leads to high overhead.

ISSN 2348 – 8034
Impact Factor- 4.022

II. RELATED WORK

To enhance the security of data communications various cryptographic algorithms are applied to smart grid.Among symmetric and asymmetric ciphers,symmetric cipher handles large amounts of data more efficiently, but often has a shorter lifespan.[12] However, this becomes an important challenge in SG, due to millions of wide-spread entities. [1]

The electric power industry needs to remain vigilant to ensure energy efficiency, reliability, and security; in the transition to renewable sources of energy; reduce greenhouse gas emissions; and build a sustainable economy that ensures future prosperity. The three-volume report, Guidelines for Smart Grid Cyber Security, presents an actionable initial analytical framework that organizations can use to develop effective cyber security strategies and solutions tailored to their particular combinations of Smart Grid-related characteristics, risks, and vulnerabilities. The asymmetric encryption is applied to meet the specific requirements of the security of Zigbee network. Nguyen and Rong employ the identity-based cryptography to secure ZigBee communication. [2] The sender uses the receiver's identification as the public key to encrypt the message; the receiver obtains the corresponding private key from the private key generator to decrypt the message.

ZigBee is a specification of defining a set of protocols and architecture for monitoring and control networks. With the advantages of high availability, low cost and low Smart grid deals with the development of a new class of sensors called the smart "stick-on" sensors. These are low cost, self-powered, universal sensors that provide a flexible monitoring solution for grid assets. These sensors can be mass deployed due to low cost, need low maintenance as they are self-powered, and can be used for monitoring a variety of grid assets, power consumption, ZigBee are ideal for both residential and industrial settings. The grid to be operated on requiring a significant dependence on distributed intelligence and broadband communication capabilities. Public key infrastructure (PKI) supported by other architectural components, was considered the best overall solution for smart grid. [3]

PKI is considered as the basis of most effective key management solution in smart grid. The management of the encryption key is a challenging and necessary issue in utilizing cryptographic algorithms for the smart grid.[4]The details of the network architecture, interoperability and integration, and different design aspects of the stick-on sensor, such as novel energy harvesting techniques, power management, wide operating range, and reliability are taken care by this technology. Solving the network problem using real time location based Dijkstra's algorithm is problematic because of complicated structure. To protect the home area network (HAN) and security of advanced metering infrastructure, a secure data aggregation and dispatch scheme is proposed. The orthogonal chip code is employed to keep the confidentiality and anonymity for collecting the reading-data of smart home devices to the household smart meter and for distributing the control message[5].

The smart meters, which are distributed at different hierarchical networks of the SG can first achieve mutual authentication and establish the shared session key with Diffie-Hellman exchange[6]. The hash based authentication is used to authenticate the subsequent messages. Its advantages are the security factors with respect to the fact that solving the discrete logarithm is very challenging, and that the shared key (i.e. The secret is never itself transmitted over the channel. There are expensive operations involved and the algorithm cannot be used to encrypt messages it can be used for establishing a secret key.

A novel key management scheme which combines symmetric key technique and elliptic curve public key technique. The symmetric key scheme is based on the Needham-Schroeder authentication protocol. The goal of this work is to propose an efficient and scalable key management protocol for secure unicast, multicast, and broadcast communications in a smart grid network with millions of entities.
But all these methods rely on a third party for identity authentication or key generation. It might cause additional equipment cost and communication traffic. [7]

ISSN 2348 – 8034
Impact Factor- 4.022

III. OBSTACLES IN A SMART GRID NETWORK

In spite of the fact that the deployment of smart grids is enormously beneficial, several security and privacy concerns arise. An attacker could possibly intercept traffic going to the central system, send commands to the smart meters or inject code into the backend control system. Security for such systems involves both key management on a scale involving a large number of credentials and keys, and local cryptographic processing on the sensors such as encryption and digital signatures. Most terminal devices in smart grid are connected into the intranet, such as smart sensors and intelligent applications. It is believed that the malicious users could not access them without the intranet and Mac address of these devices. In our experiments, the Adversary obtains the address of the smart meter by monitoring their communication and then injects the false data into the meter.

In a network of smart grids, a packet drop attack or black hole attack is a type of denial-of-serviceattack n which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from a number of different causes. Because packets are routinely dropped from a lossy network, the packet drop attack is very hard to detect and prevent.
The malicious router can also accomplish this attack selectively, e.g. by dropping packets for a particular network destination, at a certain time of the day, a packet every *n* packets or every *t* seconds, or a randomly selected portion of the packets. This is rather called a **gray hole attack**. If the malicious router attempts drop all packets that come in, the attack can actually be discovered fairly quickly through common networking tools such as trace route. Also, when other routers notice that the compromised router is dropping all traffic, they will generally begin to remove that router from their forwarding tables and eventually no traffic will flow to the attack. However, if the malicious router begins dropping packets on a specific time period or over every n packets, it is often harder to detect because some traffic still flows across the network.

The problem definition of this project is to enhance the security considerations of the smart grid network in two phases. First using AODV algorithm for transfer of data and to increment the efficiency of AODV(Adhoc on demand distance vector)algorithm using PTA (Path Tracing Algorithm). Then in second phase data packets are sent on a randomly selected path after encrypting with ECC algorithm.

IV. METHODOLOGY

A. AODV-PTA Algorithm

For selecting an optimized route AODV protocol follows the finding of the minimum delay path.If we add path tracing algorithm to AODV routing protocol,it will help in finding malicious nodes and also prevent formation of Black-hole tunnels in a smart grid network.PTA generally used in computer graphics for delivering images in a 3-dimensional scenes such that global illumination is loyal to reality.If each node in a smart grid is applied with PTA,which calculate per hop distance based on RTT value and finds Black-hole tunnels using frequency appearance count.

ISSN 2348 – 8034
Impact Factor- 4.022

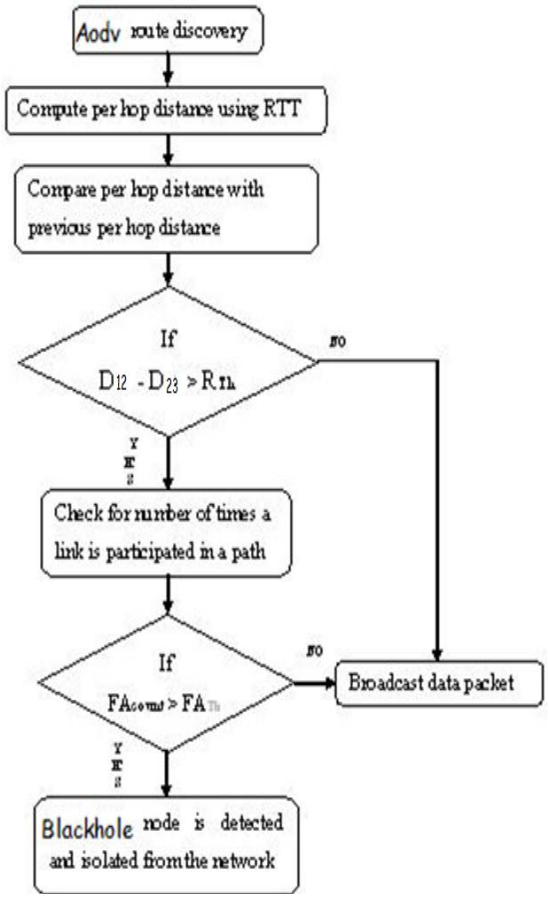

Fig1.Path Tracing Algorithm.

B. Packet Delivery using ECC Algorithm

This is the final module of the system. This specifies how a packet of data is sent from source to destination. The source node encrypts the message using the ECC algorithm. The encrypted message is transferred in data packets along the randomly selected path. Other nodes cannot see what is being transferred in the packets. Once data packets reached the destination, data's are decrypted in the destination node using the cipher key. A message sent from source is received at the destination without loss or damage to data.

C. Randomized Algorithm

Randomization algorithm is used to select a random path from the various available paths in the route table.It prevents attackers from easily predicting the path.The algorithm is as follows:

- Let Ni denotes node in a network,
- t be Destination node,
- W^{Ni} be an estimated minimal cost to send a packet to t
- Nexthop be the next node along the Minimal cost path to the destination node
- C_t^{Ni} be a set of node candidates for the nexthop
- H_t^{Ni} be a set of tuples, records the history for packet deliveries through the node Ni to the destination node t.

Randomization Procedure:

RANDOMIZEDSELECTOR (s,t, pkt)
Let h_s be the used nexthop for the previous packet
delivery for the source node s.
if$h_s \varepsilon C_t^{Ni}$ then
if $|C_t^{Ni}| > 1$ then Randomly choose a node x from $\{C_t^{Ni} - h_s\}$ as a nexthop, and send the packet*pkt* to the node x.
h_s x, and update the routing table of Ni.
else
Send the packet*pkt* to h_s.
endif
Else
Randomly choose a node y from C_t^{Ni}
As a nexthop, and send the packet*pkt* to the node y.
h_s y, and update the routing table of Ni.
end if

V. EXPERIMENTS AND ANALYSIS

Various experiments are conducted to show how the security of the smart grid is enhanced is presented in this section.

A. Packet delivery ratio:

The ratio of the number of delivered data packets to the destination. This illustrates the level of delivered data to the destination.

∑ Number of packets receive / ∑ Number of packets send

The greatest value of the packet delivery ratio means better performance of the protocol.Perl analysis is conducted to count the number of data packet sent, datapacket received and delivery ratio before implementation of path tracing algorithm which is 79.779 as depicted in fig1.The data packet delivery ratio after implementation of path tracing algorithm is 89.531 as depicted in fig2.But after implementation of path tracing with ECC algorithm the packet delivery ratio is 93.150.

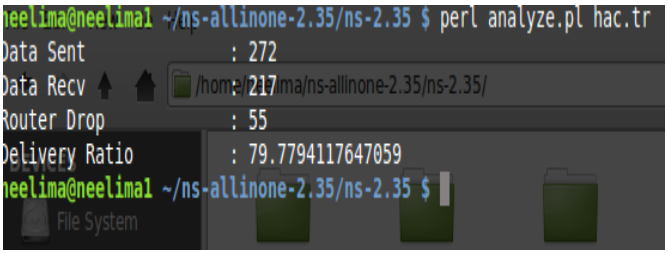

Fig2.Perl analysis of Packet Delivery Ratio before applying PTA.

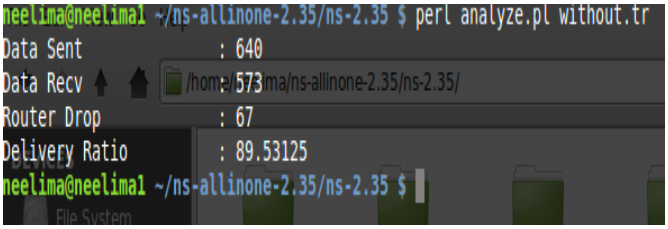

Fig3.Perl analysis of Packet Delivery Ratio after applying PTA

ISSN 2348 – 8034
Impact Factor- 4.022

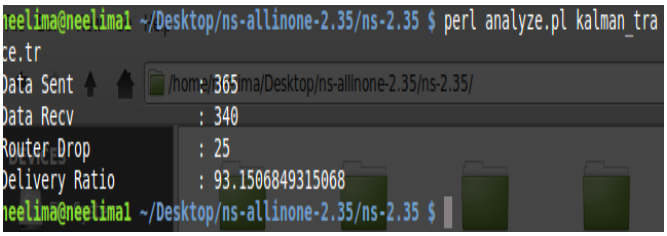

Fig4.Perl analysis of Packet Delivery Ratio after applying ECC.

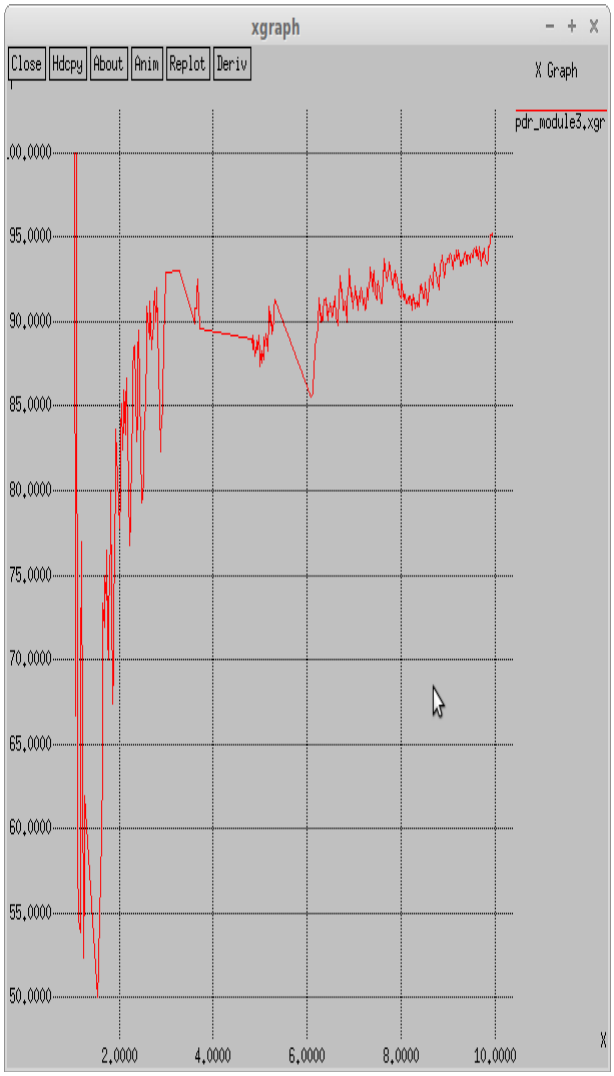

Fig5.Graph depicting Packet delivery Ratio where x-axis denotes normal time in ms and y-axis denotes delivery ratio.

B. End-to-end Delay:

The average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

ISSN 2348 – 8034
Impact Factor- 4.022

∑ (arrive time – send time) / ∑ Number of connectionsThe lower value of the end to end delay means better performance of the protocol.

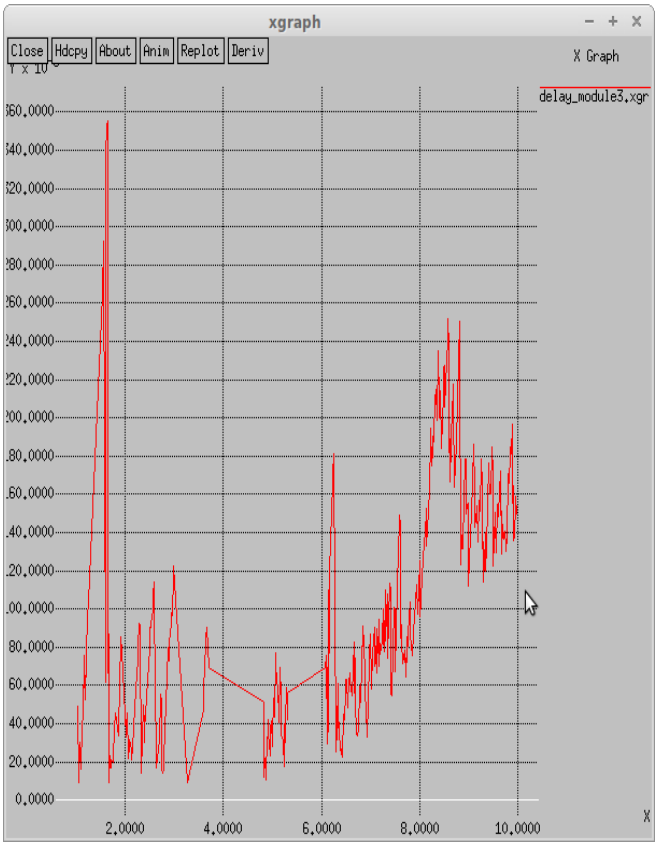

Fig6. Depicting the delay with x-axis denotes normal time and y-axis denotes delay in millisecs.

C. Throughput:

Throughput isthe amountof datareceived bythedestination.The Average Throughput is the throughput per unit of time.

Example:Suppose a TCP receiver receives 60 M Bytes of data in 1 min, then the throughput of the period is 60 M Bytes.The average throughput is 60 M Bytes/min or 1 M Bytes/sec

ISSN 2348 – 8034
Impact Factor- 4.022

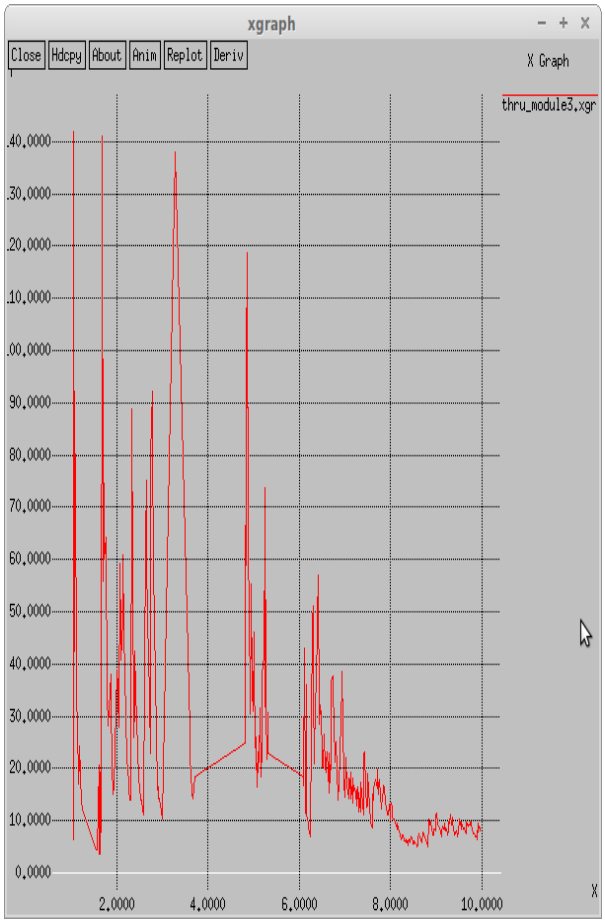

Fig 6.depicts the throughput with x-axis denotes normal time and y-axis denotes delivery packets.

VI. CONCLUSION

In this paper a 3-stage security is applied to the network of smart grid.In the first stage AODV with PTA is applied to secure the nodes in smart grid from formation of Black-hole tunnels.In the second stage data packets are encrypted with ECC algorithm making the messages 100% secure.And finally in the third stage data packets are sent in a randomly selected path using Randomized algorithm.

REFERENCES

1. *The Smart Grid Interoperability Panel Cyber SecurityWorking Group, "Introduction to NISTIR 7628 guidelines for smart grid cyber security," 2010 [Online]. Available: http://www.nist.gov/smartgrid/upload/ nistir-7628_total.pdf.*
2. *S. Nguyen and C. Rong, "ZigBee security using identity-based cryptography autonomic and trusted computing," in Proc. 4th Int. Conf. Autonomic Trusted Comput. (ATC'07), 2007, vol. 4610, Lecture Notes in Computer Science, pp. 3–12.*
3. *A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," IEEE Trans. Smart Grid, vol. 1, pp. 99–107, 2010.*
4. *R.Moghe, F. C. Lambert, and D. Divan, "Smart "Stick-on" sensors for the smart grid," IEEE Trans. Smart Grid, vol. 3, pp. 241–252, 2012.*
5. *Y. Ye, Q. Yi, and H. Sharif, "A secure data aggregation and dispatch scheme for home area networks in smart grid," in Proc. 2011 IEEE Global Telecommun. Conf., pp. 1–6.*

6. *M. M. Fouda, Z. M. Fadlullah, N. Kato, L. Rongxing, and S. Xuemin, "A lightweight message authentication scheme for smart grid communications," IEEE Trans. Smart Grid, vol. 2, pp. 675–685, 2011.*
7. *]W. Dapeng and Z. Chi, "Fault-tolerant and scalable key management for smart grid," IEEE Trans. Smart Grid, vol. 2, pp. 375–381, 2011.*
8. *L. Rongxing, L. Xiaohui, L. Xu, L. Xiaodong, and S. Xuemin, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," IEEE Trans. Parallel Distrib. Syst., vol. 23, pp. 1621–1631, 2012*
9. *H. Li, S. Gong, L. Lai, Z. Han, R. Q. Qiu, and D. Yang, "Efficient and secure wireless communications for advanced metering infrastructure in smart grids," IEEE Trans. Smart Grid, vol. 3, pp. 1540–1551, 2012.*
10. *X. Sheng, G.Weibo, and D. Towsley, "Secure wireless communication with dynamic secrets," in Proc. 2010 IEEE INFOCOM, pp. 1–9. P. Jokar,H. Nicanfar, and V. C. M. Leung, "Specification-based intrusion detection for home area networks in smart grids," in Proc. 2011 IEEE Int. Conf. Smart Grid Commun. (SmartGridComm), pp. 208–213.*
11. *P. Jokar,H. Nicanfar, and V. C. M. Leung, "Specification-based intrusion detection for home area networks in smart grids," in Proc. 2011 IEEE Int. Conf. Smart Grid Commun. (SmartGridComm), pp. 208–213.*
12. *The Smart Grid Interoperability Panel Cyber SecurityWorking Group, "Introduction to NISTIR 7628 guidelines for smart grid cyber security," 2010 [Online]. Available: http://www.nist.gov/smartgrid/upload/ nistir-7628_total.pdf.*
13. *S. Nguyen and C. Rong, "ZigBee security using identity-based cryptography autonomic and trusted computing," in Proc. 4th Int. Conf. Autonomic Trusted Comput. (ATC'07), 2007, vol. 4610, Lecture Notes in Computer Science, pp. 3–12.*