NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 3, ISSUE4, APR.-2016

GPSR ALGORITHM TO OVERCOMETHE LIMITATIONIN PUBLIC KEY INFRASTRUCTURE FOR SECURITY IN SMART GRID COMMUNICATION

Nita Jadhav
Department of Computer Engineering,
SCEMR, Savitribai Phule Pune University.

Shyam Gupta
Department of Computer Engineering,
SCEMR, Savitribai Phule Pune University.

ABSTRACT

Smart grid communication is the generic label for the application of the computer intelligence and networking abilities. Smart grid adds new functionalities to electrical power systems. Because of this, many security problems arises. For security in small grid communication, many types of protocols and infrastructures use their own set of security requirements. Public key infrastructure is one of the solutions for ensuring security in the smart grid communication. Although PKI is viable solution, it has some difficulties to satisfy the requirements in availability, privacy preservation and scalability. The wireless mesh network technology is the promising infrastructure solution to support smart functionality, scalability, as well as it can provide redundant routes for the smart grid communication network to guarantee the network availability. Greedy perimeter stateless routing algorithm is useful in wireless mesh network technology to overcome the limitations that occurs in the public key infrastructure for the security in smart grid communication.

KEYWORDS - PKI, GPSR algorithm, IP algorithm for object tracking.

INTRODUCTION

Smart Grid is recognized as two way communication technology. There is numerous Communications, intelligent, monitoring and electrical elements employed in power grid that makes it smart. These elements regularly generates cum real timely talks the critical information like monitoring data, customer energy consumption, grid status, demand response etc among the smart grid devices. The sections of the chapter are organized as follows. Section ‘A’ presents background. Security and privacy in smart grid is discussed in section B.

A. BACKGROUND

Smart grid is an upgrade to the power generation and distribution that dynamically integrate power regeneration [1]. The two way communication technology is called smart grid. It involves

employment of communication cum information system with power infrastructure, enabling monitoring, inculcating demand response activities among energy producers and consumers which significantly increase efficient utilization of the power. The Smart Grid employs millions of devices forming networked together, and the crucial aspect is the security, integrity, privacy of these individual devices is important to ensure whole stability of the power infrastructure. There are many smart meters employed in smart grid forming AMI network. These meters generate critical information in bulk that must be prevented from attacks or manipulations.

B. SECURITY AND PRIVACY IN SMART GRID

Security is a challenging game of wits, pitting security attackers versus assets holders. Security in SG is of no exception to this paradigm. Cyber security is intended as one of the crucial challenges for SG. In Figure 1.1 shows the classification of the function on security and privacy for SG [2].

Security in Smart Metering: The security issues arrive from the recently deployed smart meters in large quantity. Smart meters are very attractive point for malicious hackers. Hackers or attackers who compromise a smart meter can immediately alter their energy costs or change generated energy meter readings to make money. A common consumer cheating in traditional power grid is that customers turn a physical meter upside down inside the electrical socket so as to cause the internal usage encounters to run backward. Due to the usage of smart meter, such attack can even be done with remote PCs. Moreover, wide usage of smart meters may provide a potentially many number of opportunities for adversaries. For example, inserting false information could mislead the electric utility into making incorrect decisions about region or local usage and capacity.

Privacy in Smart Metering: Smart meters in AMI also have unintended outcomes for customers privacy. NIST found out that the big benefit given by the SG, i.e. the ability to get richer data to and from consumer meters and other electric appliances, is also its Achilles heel from a privacy viewpoint. The more obvious privacy trouble is that the power usage information stored in the meter reacts as an information-rich side channel, and can be reused by interested groups to get personal data like consumer energy usage habits, behaviours, activities, likings, and even beliefs.

Security in Monitoring and Measurement: High deployment of monitoring and measurement devices (e.g. sensors, Meters and PMU should also give rise to system vulnerabilities. The effective functioning of SG is widely dependent on the widely-deployed accurate measurement devices. Such measured information is typically transmitted to a control utility centre, such as Supervisory Control and Data Acquisition Systems. State estimators in the utility centre estimate the power grid status by analysing the measurement data and power system models. Therefore, it is very vital to guarantee the integrity of the data in SG. A usual attack to corrupt data integrity is the stealth attack.

INFORMATION TRANSMISSION

Security attacks on information transmission in SG can be classified in three major types-

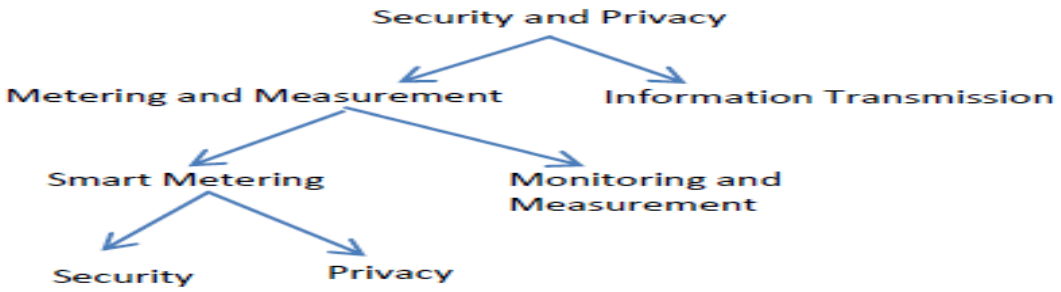

Figure 1.1: Classification function on security and privacy for SG

Network Availability: Malicious attacks on intending network availability can be called as DoS attacks. They attempt to slow down, block, or even manipulate information transmission so as to make network resources unavailable to terminals that are in need to exchange information in SG.
Data Integrity: Data integrity attacks generally intend to deliberately manipulate or corrupt information shared within the SG, its elements and may be highly damaging in the SG
Privacy of Information: Information privacy attacks just intend to eavesdrop on communications in SG elements so as to acquire desired information, like consumer account number and their energy usage.

SMART GRID COMMUNICATION BASICS AND ANALYSIS

One important feature of the smart grid is the integration of high-speed, reliable and secure data communication networks to manage the complex power systems effectively and intelligently. The communication architectures to be used in the smart grid provide the platform to build the automated and intelligent management functions in power systems. The functional requirements of communication architectures depend on the expected management tasks.

A. SMART GRID COMMUNICATION ARCHITECTURE

The communication infrastructure in smart grid must support the expected smart grid functionalities and meet the performance requirements. As the infrastructure connects an enormous number of electric devices and manages the complicated device communications, it is constructed in a hierarchical architecture with interconnected individual sub networks and each taking responsibility of separate geographical regions.

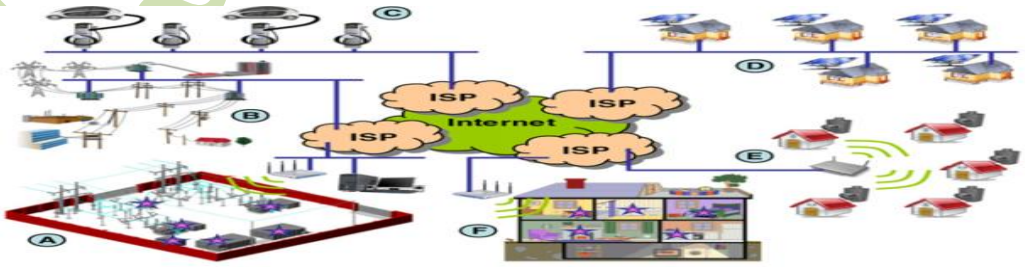

Figure 2.1: An example of communication architecture in SG

Wide area networks: Wide area networks form the communication backbone to connect the highly distributed smaller area networks that serve the power systems at different locations. When the control centres are located far from the substations or the end consumers, the real-time measurements taken at the electric devices are transported to the control centres through the wide area networks and, in the reverse direction, the wide area networks undertake the instruction communications from control centres to the electric devices. The wide area networks also convey communications between the IEDs and the control centres. The IEDs are installed along transmission lines and in substations to capture local SCADA information and act upon the control and protection commands from the control centres. Moreover, to support the reception of high speed PMU data at the control centres, a high bandwidth network is required. Currently, the substations communicate with the control centres using point to point telephone or microwave links. Thus in the absence of high speed network, the sensed digital data from PMUs is only limited inside substations and cannot be effectively utilized by the control centres. Figure 2.1 illustrates the An example of communication architecture in smart grid [3].

Field area networks: Field area networks form the communication facility for the electricity distribution systems. The electrical sensors on the distribution feeders and transformers, IED devices capable of carrying out control commands from DMS, DERs in the distribution systems, PEV charging stations and smart meters at customer premises form the main sources of information to be monitored and controlled by the DMS at the control centres. The power system applications operating in the distribution domain utilize field area networks to share and exchange information. These applications can be categorized as either field based (related to transmission lines, sensors, voltage regulators, etc.) or customer based (related to end customers, like houses, buildings, industrial users, etc.). Field based applications include OMS, SCADA applications, DER monitoring and control, etc. Customer based applications include AMI, DR, LMS, MDMS, etc. These two classes of applications operating in the distribution domain have different critical requirements.

Home area networks: Home area networks are needed in the customer domain to implement monitoring and control of smart devices in customer premises and to implement new functionalities like DR and AMI. Within the customer premises, a secure two-way communication interface called ESI acts as an interface between the utility and the customer[4]. The ESI may support different types of interfaces, including the utility secured interactive interface for secure two way communications and the utility public broadcast interface for one-way receipt of event and price signals at the customer devices. The ESI may be linked (either be hardwired or through the home area networks) to a smart meter capable of sending metering information. This information is communicated to the utility. The ESI also receives RTP from the utility over the AMI infrastructure and provides it to the customers. The customers may use a display panel (called IHD) linked to the ESI or a web-based customer EMS (residing in the smart meter, an independent gateway, or some third party) and respond to pricing signals from the utility. The ESI and smart devices provide utility with the ability to implement its load-control programs by accessing the control-enabled devices at the customer site.

B. COMMUNICATION REQUIREMENT

The communication infrastructure in smart grid undertakes important information exchange responsibilities, which are the foundations for the function diversified and location distributed electric power devices to work synergetic ally. Unsatisfactory communication performance not only limits the smart grid from achieving its full energy efficiency and service quality, but also poses potential damages to the grid system. To protect the smart grid and ensure optimal operation, the communication infrastructure must meet a number of requirements [5].

Network Latency: Network latency defines the maximum time in which a particular message should reach its destination through a communication network. The messages communicated between various entities within the power grid, may have different network latency requirements. For example, the protection information and commands exchanged between IEDs in a distribution grid will require lower network latency than the SCADA information messages exchanged between electrical sensors and control centres. Moreover, the messages exchanged can be event driven (e.g., protection and control related) or periodic (e.g., monitoring related).

Data delivery critically: The protocol suite used for a particular power system application must provide different levels of data delivery criticality depending on the needs of the application. This need may be decided at the time of connection establishment between two applications. The following levels of data delivery criticality may be used:
(a) High is used where the confirmation of end-to-end data delivery is a must and absence of confirmation is followed by a retry. For example, this may be used for delivery of SCADA control commands for settings and changes of switch gear position;
(b) Medium is used where end-to-end confirmation is not required but the receiver is able to detect data loss, e.g., measured current and voltage values and disturbance recorder data;
(c) Non-critical is used where data loss is acceptable to the receiver. In this case reliability can be improved by repetitive messages. For example, this may be used for periodic data for monitoring purpose.

Reliability: The communicating devices in the power grid rely on the communication backbone in their respective domains to send and receive critical messages to maintain the grid stability. Hence, it is extremely important for the communication backbone to be reliable for successful and timely message exchanges. The communication backbone reliability is affected by a number of possible failures. These failures include time-out failures, network failures, and resource failures. A time-out failure occurs if the time spent in detecting, assembling, delivering and taking action in response to a control message exceeds the timing requirements. A network failure occurs when there is a failure in one of the layers of the protocol suite used for communication. For example, a routing protocol failure might prevent a message from reaching its destination in spite of existence of a physical link. Noise and interference in the physical medium may also disrupt the communication. A resource failure implies failure of the end node which initiates communications or receives messages. Hence, there is a need to assess the reliability of the system in its design phase and find ways to improve it.

Security: In the future power systems, an electricity distribution network will spread over a considerably large area, e.g., tens or hundreds of miles in dimension. Hence physical and cyber

security from intruders is of utmost importance. Moreover, if a wireless communication medium (like Wi-Fi or Zigbee) is used as part of the communication network, security concerns are increased because of the shared and accessible nature of the medium.

Time synchronization: Some of the devices on power grid need to be synchronized in time. The requirements for time synchronization of a device depend on the criticality of the application. Tolerance and resolution requirements for time synchronization are strict for IEDs that process time sensitive data. For example, phase measurement units (PMUs) have the strictest need of time synchronization as they provide a real-time measurement of electrical quantities (voltage and current) from across an electricity grid for analysis, measurement and control. Time synchronization can be obtained through a number of ways depending upon the resolution and jitter requirements. Precision time protocol (PTP) defined by the standard IEEE 1588 provides time synchronization with up to nanosecond precision over Ethernet networks. Global positioning system and Simple time network protocol are other ways of achieving time synchronization [6].

METHODOLOGY AND DESIGN

Security requirements of entity authentication and non-repudiation can be satisfied by employing digital signatures. Cryptographic algorithms can encrypt and decrypt data with cryptographic keys, while obtaining the keys by malicious parties can make the encryption data exposed and unauthorized manipulated.

A. EMPLOYING PKI TO SECURE SG COMMUNICATION

A PKI binds the public keys and the entities identities through the use of digital certificates. The binding is established through a registration process, and after a TA (consisting of the registration authority, certificate authority and validation authority) assures the correctness of the binding, the TA issues the certificate to the entity. Since the public key of each entity is made available to all other entities in the network, entity authentication can be achieved. In very large systems, PKI could be significantly more efficient than shared keys in terms of setting up and maintaining operational credential. This is due to the fact that each entity is only configured with its own certificate. On the other hand, when symmetric key is used, a unique key pair needs to be configured between every pair of entities. This makes key management complicated since many symmetric keys need to be maintained and the decrypting entity may not know in advance which key should be used.

B. SHORTCOMMING OF EXISTING PKI FOR USE IN SMART GRID:

Although PKI is a potential solution to secure the smart grid when compared with other approaches, it has some limitations.

Availability: In smart grid PKI, authentication on each entity consists of two steps: certificate verification and signature verification. This procedure is vulnerable to DoS attacks, because the expensive operation of scalar multiplication is involved. An adversary may keep sending fake certificate and signature to legitimate entities for preventing others from connecting to them. For example, when a smart meter authenticates other devices or smart meters, the authentication

process itself can attract attacks from distributed DoS attackers. Accordingly, a mechanism for preventing DoS attacks is needed to overcome this PKI limitation.

Scalability: The smart grid is a large system made up of many types of devices with different computational power, and different communication protocols with their own sets of security requirements. One major obstacle to provide secure communication in such a system is to ensure that the security mechanisms can be implemented in all devices, and satisfy the security requirements. Therefore, PKI should be enhanced to accommodate the different devices and security needs. The PKI also has the following protocol-level limitation.

Privacy Preservation: In order to provide identity privacy protection, an entity needs to frequently change its one-time anonymous certificate, thus each entity possesses a number of certificates. Clearly, this solution is not suitable for smart grid because preloading a large pool of certificates is not feasible for memory-limited entities. Furthermore, even though anonymous certificates in PKI can guarantee conditional identity privacy, PKI cannot support complete identity privacy preservation and privacy preservation against traffic analysis.

C. WIRELESS MESH NETWORK

WMN [5] is a new technology area that will take a hand in next generation wireless mobile networks. In contrast to traditional wireless networks, WMNs are not built on axed infrastructure. Instead of this, hosts rely on each other to keep the connection. WMNs provide low-cost broadband internet access, wireless LAN coverage and network connection to axed or mobile hosts for both network operators and users. The reason of preferring WMNs is easy, fast and deployment of the technology. A typical WMN consists of mesh routers and mesh clients. Mesh routers are axed. They have a wireless infrastructure and work with the other networks to provide a multi-hop internet access service for mesh clients. On the other hand, mesh clients can connect to network over both mesh routers and other clients. In these networks, due to large number of nodes, working through some issues like security, scalability and manageability is required. Thus, new applications of WMNs make secrecy and security mechanisms are necessities. WMN routers [7] need to have extra operation capacity to support mesh routing besides normal router duties. Thus, they have more than one network interface card. Mesh clients usually have one NIC. Because they do not require having some features like bridge and gateway. WMNs can be classified in three types- Figure 3.1 illustrates the Architecture of Wireless Mesh Network.

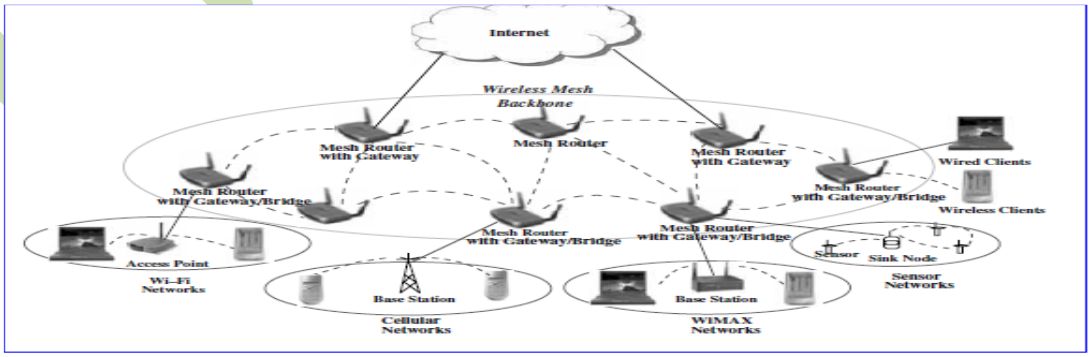

Fig 3.1 Architecture of Mesh Network.

Infrastructure or Backbone WMNs: WMNs have dozens of interconnecting clients. Connection between routers, internet and other clients is set by cables (as shown with straight lines) or wireless links as shown with dashed lines. WMN backbone mainly uses IEEE 802.11 technology within various wireless technologies.

Client WMN:A router is not necessary on the networks which are established between clients as P2P. In this case, highest level of data transmission occurs. A packet is sent to reach a destination through multi nodes. All traffic crosses over single nodes in the network. In this kind of WMNs, nodes require to have routing and self-organization functionalities.

Hybrid WMN: An additional network structure covers the existing mesh network and controls long- distance packet traffic. A hybrid WMN has infrastructure and client WMNs. While the infrastructure part provides the connection between mesh and the internet, Wi-Fi and Wi MAX networks. Client's part organizes routing processes.

IMPLIMENTATION

In Wireless mesh networks, the nodes are forwarding packets through their neighbours and this allows the packets travelling through the network scale beyond the source nodes radio range.

A. GREEDY PERIMETER STATELESS ROUTING

GPSR [8] is an on demand geographical routing protocol which uses geographical information on both source and destination nodes to calculate and determine the directional end to end path between them. In GPSR algorithm, the nodes only know one hop neighbours, which mean a node only knows the neighbours within its radio range. In such case, the algorithm is hop-by-hop algorithm which the algorithm performs the selection of its neighbour node as next hop at each node rather than the source code selects the full end to end path to the destination node. To overcome the problem of geographical routing, there are two strategies-

Greedy Forwarding: The greedy forwarding 4.1 is the typical geographical routing approach which selects all of the neighbouring nodes within the radio range and calculated their distance to destination node is selected as next hop to forward the packet. Figure illustrates example of greedy forwarding. node A is looking for the path to node D. The nodes B, C and E are the candidates of next hop for packet forwarding. The GPSR algorithm calculates the distance from destination node. In such case, node A will forward the packet to node E, then node E identify that the destination node D already within its radio range and forward the packet to node directly.

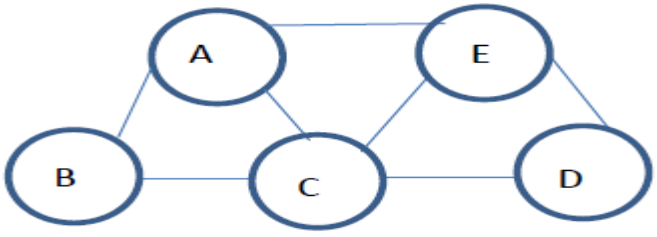

Figure 4.1: An Example of Greedy Forwarding

The void problem in Greedy forwarding: Greedy Forwarding is not working effectively in some network scenarios. For example, if there is no neighbour node which has the closer distance than the source node to the distance node. In such case, the algorithm will know which neighbour to forward.

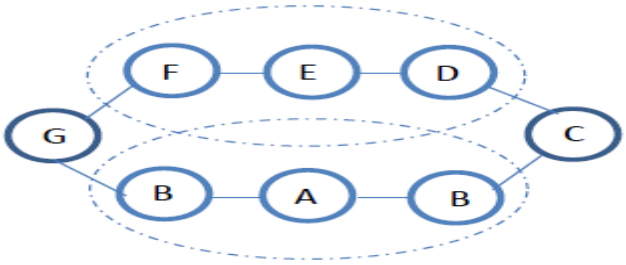

Figure 4.2: An Example of void problem in Greedy Forwarding

An Example is shown in figure 4.2. Node A is sending packets to node E. The red dash circle is the radio range of node A, and the black dash circle is the radio range of node E. The black lines are the wireless connections between the nodes. Within node A's radio range, there are two neighbours which are node H and node B. As node A wants to send packets to node E, but node H and node B both have longer path to node E than node A. In such a case, the greedy forwarding cannot select node H and node B, which indicates non-reachable to the destination node. But there are two possible paths to destination nodes H, G, F or nodes B, C, D. Therefore, the second strategy of perimeter forwarding is designed for such situation.

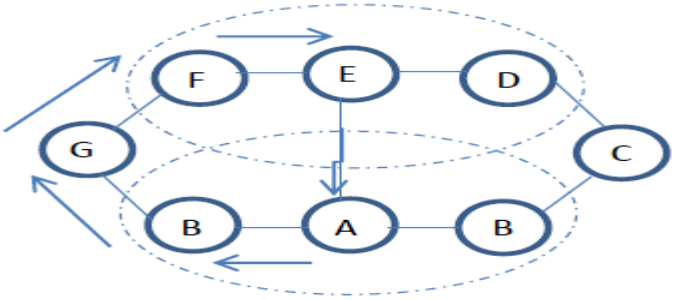

Figure 4.3: An Example of Perimeter Forwarding

Greedy Perimeter: Whenever in a situation that the source node has the closest distance to the destination node which is out of its radio range, the perimeter forwarding algorithm will be conducted. The perimeter forwarding [8] follows the right hand rule which is inspired from the real life path finding when people get lost in the maze. In GPSR, the right-hand rule is described in _g 4.3.

As shown in _g 4.3, node A wants to send packets to node E. The right-hand rule in GPSR is travelling ahead counter clock wise from the dash line between node A and node E, which is to select the first neighbouring node appeared in the counter clock wise direction to forward the packets. So the node H is selected between node A and node E, then nodes G,F until reaching node E.

CONCLUSION

Smart grid communication network requires security concerns that are network availability, information privacy and scalability. Although public key infrastructure (PKI) is a viable solution, it has some difficulties to satisfy the requirements in availability, privacy preservation, and scalability. To complement the functions of PKI, the Wireless mesh network infrastructure is one of the promising infrastructure solutions for smart grid communication. GPSR algorithm provides faster packets forwarding ratios as compared to in PKI. The perimeter forwarding follows the right hand rule which recovers the problem occurs in the greedy forwarding.

REFERENCES

[1] M. Andreoni, *A security framework for smart-grids," UFRJ COPPE", 2013.*

[2] R. K. Bhatia and V. Bodadei, *Smart grid security and Privacy: challenges, literature survey and issues," International Journal of Advanced Research in Computer Science and Software Engineering", 2014.*

[3] M. K. Wenye Wang, Yi Xu, *A survey on the communication architectures in smart grid," North Carolina State University, Raleigh NC 27606, 2011.*

[4] R. B. Emilio Ancillotti, Marco, *The role of the rpl routing protocol for smart grid communications," IEEE, 2013.*

[5] A. H. Z. Safak Durukan Odabasi, *A survey on wireless mesh networks, routing metrics and protocols," INTERNATIONAL JOURNAL OF ELECTRONICS, MECHANICAL and MECHATRONICS ENGINEERING, pp. 92{104,* 2013.

[6] C. C. Daojing He and J. Bu, *an Enhanced Public Key Infrastructure to Secure Smart Grid Wireless Communication Networks, 7th ed. IEEE, 2014.*

[7] X. W. AN F. AKYILDIZ, *A survey on wireless mesh networks," IEEE Radio Communications, 2005.*

[8] M. Xiang, *Trust-based energy aware geographical routing for smart grid communication networks," School of Computing and Mathematical Sciences, 2013.*