# A Secure Energy Routing Mechanism for Sharing Renewable Energy in Smart Microgrid

Ting Zhu*† Sheng Xiao* Yi Ping* Don Towsley* Weibo Gong*
*University of Massachusetts, Amherst, MA, USA †Binghamton University, Binghamton, NY, USA

*Abstract*—**Due to volatile and rising energy prices, smart microgrids appear to be increasingly popular. Instead of one centrally located power plant, the microgrids will rely on solar panels and wind turbines on every house sharing renewable energy among houses. How to efficiently and optimally share energy is a challenging problem. In order to efficiently share renewable energy, routing protocols in the data network are needed, which introduces another design challenge that is how to feasibly detect and defend the major attacks against routing protocols for smart microgrids. Most of the existing secure routing protocols for other networks (such as ad hoc networks) either ignore the most challenging internal attacks such as spoofed route signaling and fabricated routing messages, or have often produced inefficient security mechanisms.**

**In this paper, we develop a novel secure energy routing mechanism (SERM) for securely and optimally sharing renewable energy in smart microgrids. SERM detects most internal attacks by using message redundancy. The simulation results have demonstrated the effectiveness of our proposed secure energy routing mechanism.**

## I. INTRODUCTION

Climate change concerns, coupled with high oil prices, serious nuclear accidents, and increasing government support has resulted in the increasing demand of renewable energy that comes from natural sources such as sunlight, wind, rain, and geothermal heat. On the energy consumption side, homes and buildings consume around 41% of the energy used in the United States [1]. When energy is transmitted from power plants to end customers, more than 6.5% energy is lost [3]. To minimize transmission and distribution losses, researchers have proposed the microgrid approach by installing renewable energy sources (such as solar panels or wind turbines) on every house to provide energy supply.

Since different locations harvest energy at different rates and houses have different dynamic energy consumption patterns, energy sharing among houses is needed to efficiently and dynamically route renewable energy from a location with energy surplus to a location with energy deficit. Figure 1 shows the architecture of a smart microgrid in which each house has its own renewable energy sources. Houses are interconnected with each other with energy routers for energy sharing. Each house is attached to a single energy router. Energy flows from one house to another through these routers.

In a smart microgrid, how to efficiently and optimally share energy among houses is a challenging problem. Although there is an extensive literature addressing the power flow optimization problem, the proposed approaches always assume that the direction of power flow is from a power station to customers. However, in a smart microgrid, a power flow can flow from any house to any other house. In other words, power flows is bidirectional and changing dynamically.

In order to share energy efficiently and optimally, each house needs to know how much extra renewable energy it can provide to (or receive from) the other houses and where it can receive (or provide) energy. This energy information is exchanged among energy routers in data network. To reduce deployment, wiring, and maintenance cost, wireless communications are used in such data network. However, wireless links are susceptible to attacks. How to design a secure routing protocol becomes a very important problem.

The attacks against routing protocols come from both outside and inside the network. In an external attack, a malicious router does not participate in the routing process but masquerades as a trusted router. It can either advertise false routing information or generate a flood of spurious service requests (such as a denial-of-service attack). While in an internal attack, the router is compromised or misconfigured and exhibits any number of different misbehaviors, such as advertising false energy sharing information, failing to report security violations of a neighboring router, misrouting packets to a non-existing router, redirecting energy to a non-optimal route, fabricating, modifying or simply dropping data packets that include energy information.

In this paper, we designed a secure energy routing mechanism. Similar to traditional routing protocols, at the control plane, energy routers securely exchange energy information of each houses in the data network and try to find the most energy efficient path on the energy network to share energy among houses. Different from traditional routing protocols, our routing mechanism has energy plane and does not have data plane. After energy routers find the most energy efficient path at the control plane on data network, energy flows from one house to another house through the most energy efficient path at the energy plane on energy network. The main contribution of this paper is as follow:

- We develop a novel mechanism that can detect most internal attacks by using message redundancy, which is required for the robustness of secure routing mechanisms with collusion detection capability.
- We propose a distributed optimal energy request algorithm and prove that this algorithm enables optimal energy sharing in smart microgrid.
- We design a secure routing mechanism that ensures message integrity and detects major internal attacks such as

978-1-4577-1702-4/11/$26.00 ©2011 IEEE

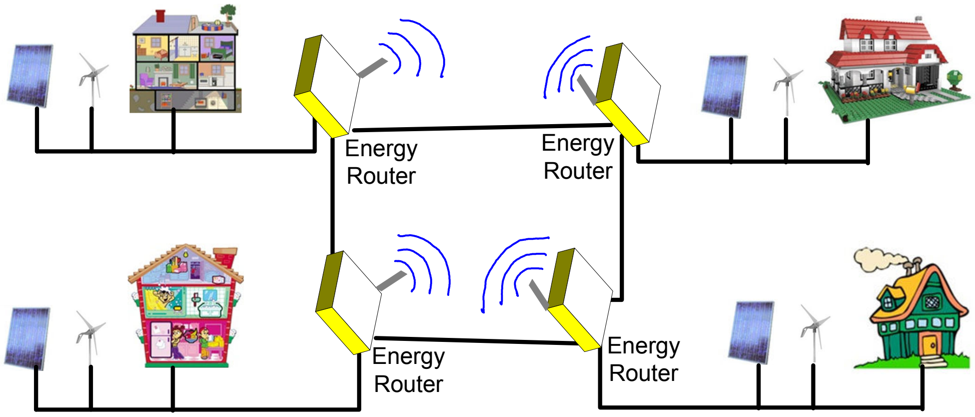


Fig. 1. Architecture of Smart Microgrid with Energy Router

spoofed route signaling and fabricated routing messages.

The paper is organized as follows. We discuss related work in Section II, introduce our secure energy routing mechanism (SERM) in Section III, analyze the robustness of SERM in Section IV, present simulation result in Section V, and conclude this paper in Section VI.

## II. Related Work

Energy harvesting, conservation and management is an intensively studied area. Many solutions have been proposed at physical layer [5], [18], link layer [6], [31], network layer [14], [12], and adaptation layer [9]. However, energy sharing in a smart microgrid is a relatively new concept, the corresponding secure routing protocols have not been designed. However, many secure routing protocols have been proposed in ad hoc networks to detect and defend against specific attacks [8], [10], [11], [13], [37], [15], [17], [26]. Based on the security mechanisms a protocol has used or the specific attacks the protocol defends against, existing secure routing protocols can be roughly divided into two categories.

The common practice among the first category is to secure the popular on-demand routing protocols, such as AODV [19] and DSR [20], by using a security association between the source and destination routers. In [21], Hu et al, based on DSR, proposed a secure routing protocol called Ariadne, by using efficient symmetric cryptography. Routing messages are authenticated by shared secrets between each pair of routers. The broadcast authentication scheme used in Ariadne is TESLA [25], which requires only loose time synchronization. In [27], the authors proposed a proactive secure routing protocol, called SEAD, based on DSDV [28] by using one-way hash chains to provide authentication to defend against attacks that modify routing information broadcasts and replay attacks but not wormhole attacks. In [22], the authors secured the on-demand protocols AODV and DSR by using digital signatures to provide end-to-end authentication.

Secure routing protocols belonging to the second category focus on protecting routing traffic against all sorts of Byzantine attacks. In [29], [30], Awerbuch, et al proposed to detect Byzantine behaviors by using a probing technique, which uses a binary search on a path to locate the faulty link. In [33], the authors proposed a secure routing protocol against Byzantine failures based on source routing and destination acknowledgements. Each packet is authenticated at each router by using MACs based on pair-wise secret keys. Digital signatures are used for the initial key setup. The faults are detected on a per packet basis to defend Byzantine adversaries.

We conclude for the above review that most secure routing protocols deal with a single source and destination pair. However, in energy sharing networks, a house may need to request energy from multiple neighboring houses. Moreover, the available energy in each house changes over time. Therefore, we need a distributed secure routing mechanism for sharing energy among houses.

## III. Secure Energy Routing Mechanism

The design of a secure energy routing mechanism contains secure key management, energy discovery packet dissemination, energy route reply packet propagation, and energy route request.

### A. Secure Key Management

In order to authenticate the routers in a network and verify the integrity of the routing information routers exchange with their neighbors, an essential component in the security architecture is the key management mechanism. In this paper, we assume that each router has an initial public/private key pair issued by a public key infrastructure (PKI) or some other certificate authority (CA) when the routers are deployed. Initially, every router $r$ receives a certificate from the CA: $T$ as follows:

$$T \rightarrow r : cert_r = \{IP_r, K_{r+}\}K_{T-}, K_{T+} \tag{1}$$

The certificate contains $r$'s IP address ($IP_r$), $r$'s public key ($K_{r+}$), and $T$'s public key ($K_{T+}$). To avoid unauthorized participation, router $r$ only exposes a part of the certificate which is encrypted by $T$'s private key (i.e., $\{IP_r, K_{r+}\}K_{T-}$). We use $cert_r^-$ to denote this part. Table I summarize our notation.

### B. Energy Discovery Packet Dissemination

The secure energy routing mechanism is an on-demand mechanism. When a house $H$ requires renewable energy from the other houses inside the microgrid, $H$'s corresponding router (assume $i$) constructs a message $m_i$ as follows:

TABLE I
NOTATIONS

| | |
|---|---|
| $K_{r+}$ | Public key of router $r$. |
| $K_{r-}$ | Private key of router $r$. |
| $\{d\}K_{r+}$ | Encryption of data $d$ with key $K_{r+}$. |
| $\{d\}K_{r-}$ | Encryption of data $d$ with key $K_{r-}$. |
| $cert_r$ | Certificate belonging to router $r$. |
| $cert_r^-$ | $r$'s encrypted part of certificate. |
| $N_r$ | Nounce issued by router $r$. |
| $IP_r$ | IP address of router $r$. |
| $P_r$ | Routing packet send out by router $r$. |
| $R_r$ | Requested energy by router $r$. |

$$m_i = [R_i, IP_i, N_i] \tag{2}$$

Where $R_i$ is the requested amount of energy required by house $H$, $IP_i$ is router $i$'s IP address, and $N_i$ is a sequence number. Then router $i$ encrypts message $m_i$ using $i$'s private key $K_{i-}$ and broadcasts the energy discovery packet ($EDP_i$) as follows:

$$i \rightarrow broadcast : EDP_i = \{m_i\}K_{i-}, cert_i^-, m_i \tag{3}$$

Since router $i$'s encrypted certificate ($cert_i^-$) is also included in the packet, only routers certified by $T$ can decrypt $K_{i+}$ from $cert_i^-$ and then use $K_{i+}$ to decrypt the encrypted version of $m_i$, which is encrypted by $K_{i-}$. In this way, we avoid the participation of routers not authorized by certificate authority $T$. Both the original $m_i$ and its encrypted version $\{m_i\}K_{i-}$ are sent out so that intermediate routers can verify whether $m_i$ has been modified during the energy discovery phase.

When the intermediate router $j$ receives the energy discovery packet from router $i$, $j$ first verifies whether $m_r$ and $\{m_i\}K_{i-}$ match. If they do not match, $j$ notifies $i$ about the mismatch. By doing this, $j$ avoids intended misbehavior by $i$. After receiving the correct $m_i$ and $\{m_i\}K_{i-}$ from $i$, $j$ checks whether the house attached to it has extra energy to share with $i$. If $j$ has sufficient energy to share with $i$, $j$ generates message $m_j$, which includes the amount of available energy and its IP address:

$$m_j = [E_j, IP_j] \tag{4}$$

Then, $j$ sends out an energy reply packet $EREP_j$, which contains the encrypted $EDP_i$ and $m_j$, $j$'s certificate, and the original $m_j$ message, shown as follows:

$$j \rightarrow broadcast : EREP_j = \{EDP_i, m_j\}K_{j-}, cert_j^-, m_j \tag{5}$$

If $j$ does not have enough extra energy, $j$ updates its requested energy $R_j = R_i - E_j$ and generates its own message $m_j$ as follows:

$$m_j = [R_j, IP_j] \tag{6}$$

Then, $j$ encrypts message $m_j$ by using its own private key $K_{j-}$, attaches the encrypted message together with its certificate and the original message $m_j$ to the received $EDP_i$ to form a new packet $EDP_j$, and then rebroadcasts $EDP_j$ (shown below).

$$j \rightarrow broadcast : EDP_j = \{EDP_i, m_j\}K_{j-}, cert_j^-, m_j \tag{7}$$

When $j$'s next hop neighbor $j+1$ receives $EDP_j$, $j+1$ will first verify whether $m_i$ and $\{m_i\}K_{i-}$ match. If they do not match, $j+1$ treats $j$ as untrustworthy. This is because $j$ should have already verified the correctness of $m_i$ and $\{m_i\}K_{i-}$ before forwarding the packet to $j+1$. If $m_i$ and $\{m_i\}K_{i-}$ match, $j+1$ further verifies whether $m_j$ and $\{m_j\}K_{j-}$ match. If they do not match, $j+1$ notifies $j$ about the mismatch. By doing this, $j+1$ ensures that $j$ acts correctly. If $j$ does not correct the mismatch, $j+1$ marks $j$ as an untrustworthy router. Here, we use redundant messages to verify the misbehavior of the intermediate routers.

After the message verification, $j+1$ checks whether its extra available energy $E_{j+1}$ is more than $j$'s requested energy $R_j$ which is the difference between $i$'s requested energy and $j$'s extra available energy (i.e., $R_i - E_j$). If $E_{j+1} < R_j$, $j+1$ constructs the energy discovery packet $EDP_{j+1}$ by attaching $\{m_{j+1}\}K_{j+1-}, cert_{j+1}^-, m_{j+1}$ to the end of $EDP_j$ packet and sends out $EDP_{j+1}$. If $E_{j+1} > R_j$, $j+1$ constructs the energy route reply packet $EREP_{j+1}$ by attaching $\{m_{j+1}\}K_{j+1-}, cert_{j+1}^-, m_{j+1}$ to the end of $EREP_j$ packet and sends out $EREP_{j+1}$.

### *C. Energy Route Reply Packet Propagation*

As discussed in the previous subsection, energy route reply (EREP) packets are generated by routers that have more extra available energy than the energy requested by these routers' previous hop. There are two design goals in the EREP packet propagation mechanism design. The first design goal is to avoid unnecessary propagation to all routers inside the network. In order to achieve this design goal, only the router that has rebroadcasted the energy discovery packet (EDP) is eligible to forward EREP packets. No other node is eligible to forward EREP packets.

The second design goal is to avoid intermediate routers fabricating routing messages. To achieve this, each router verifies whether the original message and the encrypted message match. For example, when $j$ receives an EREP from $j+1$, $j$ verifies whether $m_{j+1}$ and $\{m_{j+1}\}K_{j+1-}$ match. If they do not match, $j$ treats $j+1$ as untrustworthy and discards the EREP packet without forwarding it. Hence, each router ensures that each message it receive is correct before forwarding it.

### *D. Energy Route Request*

After router $i$ receives the EREP, $i$ first verifies whether original messages and encrypted messages match. If they do not match, $i$ further identifies the untrustworthy router based on the mismatch. For example, in Figure 2, if $m_{j+1}$ and $\{m_{j+1}\}K_{j+1-}$ do not match, $i$ infers that $j$ is untrustworthy. This is because $j$ should notify $j+1$ about the mismatch and discard the EREP, instead of forwarding it.

If the original messages and encrypted messages match, $i$ starts to request energy from other routers. The main challenge here is to ensure minimum energy loss due to the energy

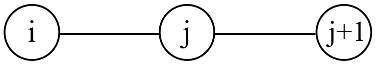


Fig. 2. Energy Route Request Example

transfer. In a loss-prone energy sharing network, the less energy transferred in the network, the less energy loss will incur during the energy transfer process. Similar to the shortest path routing in data communication networks, $i$ needs to find the minimum energy loss path between itself and other routers in the network. Specifically, given the interconnection of power cords among those routers, $i$ can derive a graph that is similar to traditional communication network graphs. In such a graph, the vertices are routers and the edges are the power cords. The weight of each edge is the efficiency of energy transfer between the pair of routers that is incident to this edge. Figure 3 shows an example of such an energy sharing network. In Figure 3, the edge labels denote the energy transfer efficiency along this edge. For example, if we assume the energy transfer efficiency ($e_{12}$) between routers 1 and 2 is 90% and the total amount of energy transferred between 1 and 2 is $1000kJ$, then the energy loss during the sharing procedure is $1000 * (1 - 0.9) = 100kJ$.

By applying any distributed shortest path algorithm [16] on such an energy sharing network, we can easily obtain the minimum energy loss path between each router and any other router in the network. Specifically, each router $i$ in the network maintains a metric called *energy sharing efficiency* for any other router $j$ in the network ($\eta_{ij}$). In Figure 3, we also show the energy sharing efficiency metric values between router 1 and any other router. For example, the minimum energy sharing efficiency between router 1 and router 4 is $e_{12} \times e_{24} = 0.81$ by going through path $1 \rightarrow 2 \rightarrow 4$. Since energy loss between routers are fixed, the minimum energy loss path only needs to be calculated when the routers are physically deployed.

Based on knowledge of the energy sharing efficiency from all other routers to router $i$, $i$ sequentially sends out encrypted energy request messages $\widetilde{m_{ij}}$ to request energy from routers with the maximal energy sharing efficiencies until it has accumulated enough energy. The detailed procedure at router $i$ is shown in Algorithm 1. Here message $\widetilde{m_{ij}}$ is encrypted by using $i$'s private key. Only routers that have already participated in energy discovery packet dissemination and received $i$'s certificate can decrypt $\widetilde{m_{ij}}$ and forward the message. If a router cannot decrypt $\widetilde{m_{ij}}$, it will not forward the message. By doing this, we avoid unnecessary and redundant transmissions. When router $j$ receives the energy sharing request from router $i$, it transfers $R_j$ energy through the minimum energy loss path to router $i$.

**Algorithm 1:** Optimal Energy Request Algorithm

```
input : Energy Request Budget $R_i$
input : Energy Sharing Efficiency ($\eta$) for other routers in the
        network with $n$ routers
Sort $\eta$ in non-increasing order ;
$j \leftarrow 2$ ;
while $R_i > 0$ OR $j \le n$ do
    Send an encrypted message
    $\widetilde{m_{ij}} = \{R_j, IP_i, IP_j, N_i\}K_{i-}$ to router $j$ that is
    corresponding to sorted $\eta_{1j}$, request energy sharing of
    $R_j$ ;
    Receive $R_j \cdot \eta_{1j}$ from the requested device ;
    $R_i \leftarrow R_i - R_j \cdot \eta_{1j}$ ;
    $j \leftarrow j + 1$ ;
```

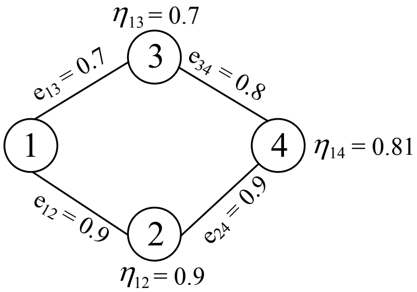
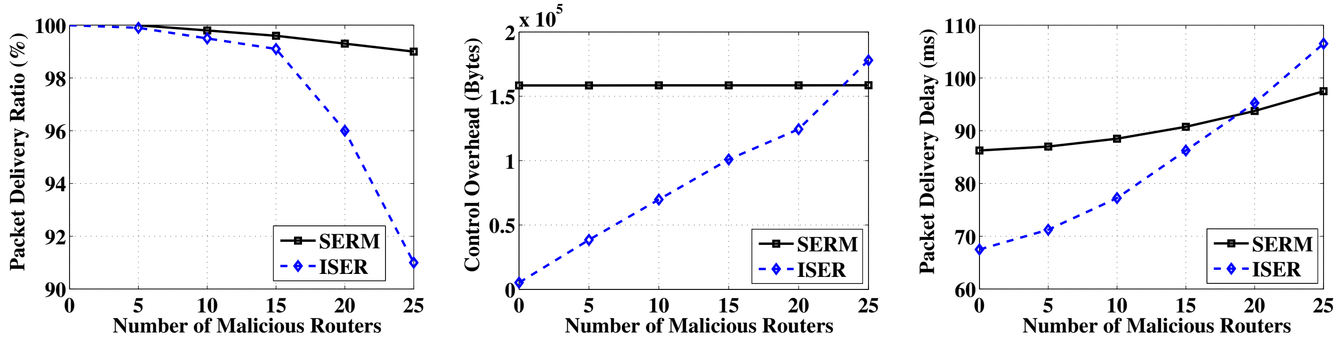


Fig. 3. Energy Sharing Network

***Proof of optimality:*** To prove the optimality of the above energy request algorithm, it is sufficient to show both the greedy choice and the optimal substructure properties. For the greedy choice property, since at each iteration we request energy from the router with the largest energy sharing efficiency to router $i$, we minimize the energy transfer loss at router $i$. This property can be proved by simple contradiction. Assume the remaining needed energy can be optimally transferred from $n$ routers, then the total energy loss $(1-\eta_{12})\cdot R_{12}+(1-\eta_{13})\cdot R_{13}+\cdots+(1-\eta_{1n})\cdot R_{1n}$ is minimal, where $R_{1j}$ is the energy transferred from router $j$ and $j = 2, \cdots, n$. If there exists a $\eta_{1,n+1}$ which is larger than $\eta_{1j}$, then accumulating energy from router $j$ can result in a greater energy loss than accumulating energy from router $n+1$ first and then from router $j$. This can be formulated as $(1-\eta_{1j}) \cdot R_{1j} > (1-\eta_{1,n+1}) \cdot R_{1,n+1} + (1-\eta_{1j}) \cdot (\frac{\eta_{1j} \cdot R_{1j} - \eta_{1,n+1} \cdot R_{1,n+1}}{\eta_{1j}})$, which contradicts the optimality claim. Consequently, the greedy choice property holds. The optimal substructure property is straightforward since after each iteration, we reduce the problem to accumulating $R_i - R_j \cdot \eta_{1j}$ amount of energy, where $R_i$ and $R_j \cdot \eta_{1j}$ are the energy budget and the energy accumulated from router $j$ at the previous iteration, respectively. By combining the above two properties, we prove that our proposed energy accumulation protocol is optimal in terms of minimum energy loss during the energy sharing process.

***Case Study:*** To further illustrate the above energy accumulation process, we provide a simple walkthrough for the energy sharing network shown in Figure 3. Assume router 1 needs to accumulate $100kJ$ from the network. First it requests energy from router 2, which has the best energy sharing efficiency, 90%, to router 1. If router 2 decides it can share $80kJ$ of energy with router 1, then router 1 would receive $80 * 0.9 = 72kJ$ from router 2. Since $72kJ < 100kJ$, router 1 would request that router 4 share $28kJ$ energy with it. Assuming router 4 can share up to $50kJ$ energy with router 1, it then will transfer $\frac{28}{0.81} = 34.6kJ$ energy to router 1, so as to meet the energy request budget at router 1 by considering energy loss during the energy sharing process.



(a) Packet Delivery Ratio

(b) Control Overhead

(c) Average Routing Acquisition Delay

Fig. 4. Impact of Malicious Routers

## IV. Security Analysis

In this section, we evaluate the robustness of SERM in the presence of different attacks.

- **Unauthorized participation**: In SERM, all packets are encrypted with the asymmetric key. Since only authorized routers have the asymmetric key, unauthorized routers are prohibited from routing control packets.
- **Spoofed Route Signaling**: In energy discovery packet and energy request packets, messages are encrypted by the original router $r$ with its private key. Only $r$ has the right key to encrypt the message. This prevents impersonation attacks.
- **Fabricated Routing Messages**: In SERM, each routing message is verified at each intermediate router. By using message redundancy, we can find out which intermediate router modified the message, we will discard that router in the routing table and prevent the fabrication of the routing messages.

## V. Simulation Results

In this section, we extensively evaluate the performance of SERM through ns-2 simulation [35]. We use the two-ray ground reflection radio propagation model. The Medium Access Control protocol used is the IEEE 802.11 Distributed Coordination Function (DCF) [36]. Since this work is the first to investigate secure energy sharing in a smart microgrid, the state-of-the-art research (e.g., secure routing protocols in ad hoc networks) is complementary, but provides no appropriate baseline for comparison. Therefore, we compare the network with secure energy sharing enabled with the same network without any encryption, referred to as the insecure energy routing (ISER) protocol. Based on NIST's guidelines for smart grid cyber security, 1024 bits RSA key length is suggested for use between 2011 and 2029 [2]. We use the 1024 bits RSA key which requires less than 0.79061 $ms$ runtime by using FPGA to do decryption [24]. However, the authors did not provide the runtime of encryption in [24]. They only described that the runtime of encryption is half of the runtime of decryption. Therefore, we add a 0.79061 $ms$ and 0.3953 $ms$ processing delay for each decryption operation and encryption operation, respectively.

In the simulation, we randomly deployed 100 routers inside a 3000m × 3000m square field and selected 5 source routers to periodically send out energy discovery packets at a rate of one every 20 minutes. Each simulation is run for 6000 seconds. Each collected data point is an average of 20 such runs.

We analyzed the impact of malicious routers by varying the number of malicious routers in the field from zero to 25. The malicious routers do not forward any control packets and periodically send out energy discovery packet without encryption every 3 minutes. Three metrics are used to evaluate the protocols:

- ***Packet Delivery Ratio***: Since the source router does not specify a destination when it send out energy discovery packets, we cannot measure the packet delivery ratio from the source router to the destination. Therefore, we define a round-trip version of the packet delivery ratio, which is the ratio of the total number of energy route reply packets received by source routers to the total number of corresponding energy discovery packets sent out by source routers. If source routers receive multiple energy route reply packets for the same energy discovery packet from multiple intermediate routers, we count only one of them.
- ***Control Overhead (bytes)***: The total amount of bytes transmitted during energy discovery packet dissemination, energy route reply packet propagation, and energy route request.
- ***Average Routing Acquisition Delay (ARAD)***: The average delay between sending an energy discovery packet (EDP) and receiving an energy route reply (EREP) packet.

Figure 4(a) compares the packet delivery ratio of SERM and ISER. When the number of malicious routers increases, the packet delivery ratios of both SERM and ISER decreases. This is because the increase in the number of malicious routers results in fewer benign routers to forward the energy discovery packets and energy route reply packets. Routers running ISER need to forward malicious routers' fake energy discovery packets, which may collide with real energy discovery packets. On the other hand, by verifying the integrity of messages, routers running SERM will not forward messages generated by malicious routers. Therefore, SERM has a higher packet delivery ratio than ISER.

Similarly, by discarding the packets received from the malicious routers, the control overhead of SERM remains stable when the number of malicious routers increases (shown in Figure 4(b)). When there are no malicious routers, ISER has less control overhead than SERM. However, routers running

ISER cannot differentiate between the malicious routers' energy discovery packets and real energy discovery packets. As a result, the control overhead of ISER proportionally increases when the number of malicious routers increases. When the number of malicious routers is 25, ISER has higher control overhead than SERM.

Figure 4(c) shows that the packet delivery delay of both SERM and ISER increases when the number of malicious routers increases. This is due to the change of route when the number of malicious routers increases. With more malicious routers and fewer benign routers, the packets may need more hops to reach the appropriate router. Therefore, the packet delivery delay increases. Moreover, routers running ISER also needs to forward fake packets. Processing and forwarding fake packets introduces extra delay, which causes ISER has longer delay than SERM when the number of malicious routers increases.

## VI. Conclusions

In this paper, we proposed a secure energy routing mechanism (SERM) to securely and optimally share energy in smart microgrids. By using message redundancies during topology discovery, SERM addressed the most challenging problem which is the detection of internal attacks.

Simulation results show that SERM is robust under different network settings. Our future work will be conducting more simulations under different network configurations. We will also compare the performance of SERM to that of other secure routing protocols.

## VII. Acknowledgements

This work was supported by NSF under grant #1019343 to CRA for the CI Fellows Project and grant CNS-1018464.

## References

[1] Energy Information Agency, "Energy Consumption," *http://www.need.org /needpdf/infobook_activities/IntInfo/ConsI.pdf.*

[2] The Smart Grid Interoperability Panel Cyber Security Working Group, "Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security," *http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf.*

[3] U.S. Energy Information Administration, *http://tonto.eia.doe.gov/tools /faqs/faq.cfm?id=105&t=3.*

[4] W. Stallings, "Cryptography and Network Security: Principles and Practice," *Prentice Hall*, 3rd Edition, 2003.

[5] T. Zhu, Y. Gu, T. He, and Z. Zhang, "eShare: A Capacitor-Driven Energy Storage and Sharing Network for Long-Term Operation," *SenSys '10.*

[6] Y. Gu, T. Zhu, and T. He, "ESC: Energy Synchronized Communication in Sustainable Sensor Networks," *ICNP '09.*

[7] R. Molva, "Internet Security Architecture," *Journal of Computer Networks*, no. 8, vol. 31, pp. 785-899, April 1999.

[8] R. Perlman, "Network Layer Protocols with Byzantine Robustness," *PhD thesis*, MIT LCS TR-429, October 1988.

[9] T. Zhu, Z. Zhong, Y. Gu, T. He and Z. Zhang, "Leakage-Aware Energy Synchronization for Wireless Sensor Networks," *MobiSys '09.*

[10] S. L. Murphy and M. R. Badger, "Badger, Digital signature protection of the OSPF routing protocol," *in Symposium on Networks and Distributed Systems Security*, 1996.

[11] R. Hauser, T. Przygienda, and G. Tsudik, "Reducing the cost of security in link-state routing," *in Symposium on Networks and Distributed Systems Security*, 1997.

[12] T. Zhu, and D. Towsley, "$E^2R$: Energy Efficient Routing for Multi-hop Green Wireless Networks," *in workshop on Green Communications and Networking*, 2011.

[13] S. Cheung, "An efficient message authentication scheme for link state routing," *The 13th Annual Computer Security Applications Conference*, pp. 9098, December 1997.

[14] T. Zhu, Z. Zhong, T. He, and Z. Zhang, "Exploring Link Correlation for Efficient Flooding in Wireless Sensor Networks," *NSDI '10.*

[15] K. Zhang, "Efficient protocols for signing routing messages," *Symposium on Networks and Distributed Systems Security*, 1998.

[16] A. G. Ciancio, S. Pattem, A. Ortega, and B. Krishnamachari. Energy-efficient data representation and routing for wireless sensor networks based on a distributed wavelet compression algorithm. In *IPSN '06.*

[17] D. Huang, A. Sinha, and D. Medhi, "A Double Authentication Scheme to Detect Impersonation Attacks in Link State Routing," *ICC '03.*

[18] Z. Zhong, T. Zhu, T. He, and Z. Zhang, "Demo: Leakage-Aware Energy Synchronization on Twin-Star Nodes," *SenSys '08.*

[19] C. E. Perkins and E. M. Royer, "Ad Hoc Networking," chapt.5, Ad hoc On-Demand Distance Vector Routing, Addison-Wesley, 2000.

[20] D. B. Johnson, D. A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks," *Ad Hoc Networking*, pp. 139-172, Addison-Wesley, 2001.

[21] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," *The 8th ACM International Conference on Mobile Computing and Networking*, September 2002.

[22] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. Belding-Royer, "Authenticated Routing for Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications* , vol. 2, no. 1, March 2005.

[23] D. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A High-Throughput Path Metric for Multi-Hop Wireless Routing", *MOBICOM*, Sept. 2003.

[24] Muhammad I. Ibrahimy, Mamun B.I. Reaz, Khandaker Asaduzzaman and Sazzad Hussain, "FPGA Implementation of RSA Encryption Engine with Flexible Key Size", *International Journal of Communications*, Oct. 2007.

[25] Perrig, R. Canetti, D. Song, and J. D. Tygar, "Efficient and Secure Source Authentication for Multicast," *Network and Distributed System Security Symposium*, NDSS01, p. 35-46, Feb. 2001.

[26] T. Zhu, and M. Yu, "A Dynamic Secure QoS Routing Protocol for Wireless Ad Hoc Networks," *Sarnoff '06*,

[27] Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," *The 4th IEEE Workshop on Mobile Computing Systems and Applications*, 2002.

[28] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," *ACM SIGCOMM94 Conference on Communications Architectures, Protocols and Applications*, 1994.

[29] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An on-demand secure routing protocol resilient to byzantine failures," *ACM Workshop on Wireless Security (WiSe)*, September 2002.

[30] B. Awerbuch, R. Curtmola, D. Holmer, and C. Nita-Rotaru, "ODSBR: An On-Demand Secure Byzantine Routing Protocol," *JHU CS Technical Report Version 1*, October 15th, 2003.

[31] A. Malvankar, M. Yu, and T. Zhu, "An Availability-Based Link QoS Routing for Mobile Ad Hoc Networks," *Sarnoff '06*

[32] D. Boneh, C. Gentry, H. Shacham, and B. Lynn, "Aggregate and verifiably encrypted signatures from bilinear maps," *Proceedings of Advances in Cryptology - Eurocrypt03*, LNCS, 2003.

[33] I. Avramopoulos, H. Kobayashi, R. Wang, and A. Krishnamurthy, "Highly Secure and Efficient Routing," *INFOCOM '04.*

[34] S. Capkkun, L. Buttyan, and J. Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," *IEEE Trans. On Mobile Computing*, vol. 2, no. 1, pp. 113, January-March 2003.

[35] K. Fall and K. Varadhan (Eds.), "The ns Manual," *http://www.isi.edu/ nsnam/ns/ns-documentation.html*, 2002.

[36] IEEE Computer Society LAN MAN Standards Committee. "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-1997.*, The Institute of Electrical and Electronics Engineers, 1997.

[37] T. Zhu and M. Yu, "A Secure Quality of Service Routing Protocol for Wireless Ad Hoc Networks," *GLOBECOM '06*

[38] J. Broch, D. Maltz, D. Johnson, Y-C. Hu, and J. Jetcheva. "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols," *IEEE/ACM MOBICOM*, pages 85-97, 1998.