BULK DATA TRANSFER WITH SECURE RELIABLE ROUTING PROTOCOL IN MULTI-HOP WIRELESS NETWORKS

Nivetha S[1], Prathiba M M[2], Roopini A J[3]

[4]***Dr.Mr.Ramesh S***, *Dept. of Information Technology, K.L.N. College of Engineering, Tamil Nadu, India*
[1, 2, 3] *Student, Dept. of Information Technology, K.L.N. College of Engineering, Tamil Nadu, India*

---***---

Abstract -*Network is a group of two or more devices that can communicate. To provide bulk data transfer by using best effort path for establishing stable and reliable routes in wireless networks. To propose BFP, routing combines payment and trust systems with a trust-based and energy-aware routing protocol. To evaluate system trust the nodes competence and reliability in relaying packets in terms of multi-dimensional trust values. Mobile Ad-hoc Network (MANET) is a consistently self-configuring, infrastructure-less network of mobile devices connected wirelessly. Since the nodes communicate with each other, they cooperate by forwarding data packets to other nodes in the network. Ad-hoc On-demand Distance Vector (AODV) is one of the most appropriate routing protocol for the MANETs. The aim of the project is to transfer bulk data using secure and reliable routing protocol using trust mechanism. Trust is the degree of reliability about other node for performing certain action by keeping track of all past transaction or interactions with nodes by direct or indirect observation. However, the communication will only be secure if the initial assumption of trust is true.*

Key Words: **Adaptive routing, trust-based, routing protocol.**

1. INTRODUCTION

A Network is defined as the group of people or systems or organizations who tend to share their information collectively for their business purpose. In Computer terminology the definition for networks is similar as a group of computers logically connected for the sharing of information or services (like print services, multi tasking, etc.). Initially Computer networks were started as a necessity for sharing files and printers but later this has moved from that particular job of file and printer sharing to application sharing and business logic sharing. Proceeding further defines computer networks as a system for communication between computers. These networks may be fixed (cabled, permanent) or temporary. A network can be characterized as wired or wireless. Wireless can be distinguished from wired as no physical connectivity between nodes are needed. Routing is an activity or a function that connects a call from origin to destination in telecommunication networks and also play an important role in architecture, design and operation of networks. It deals with more and more details related to routing and its concepts. Ad-hoc networks are wireless networks where nodes communicate with each other using multi-hop links. There is no stationary infrastructure or base station for communication. Each node itself acts as a router for forwarding and receiving packets to/from other nodes. Routing in ad-networks has been a challenging task ever since the wireless networks came into existence. The major reason for this is the constant change in network topology because of high degree of node mobility. A number of protocols have been developed for accomplish this task. Some of them are DSDV and AODV routing protocols which are explained in the forthcoming chapters.

ROUTING

Routing is the act of moving information from a source to a destination in an internetwork. During this process, at least one intermediate node within the internetwork is encountered. This concept is not new to computer science since routing was used in the networks in early 1970's. But this concept has achieved popularity from the mid-1980's. The major reason for this is because the earlier networks were very simple and homogeneous environments; but, now high end and large scale internetworking has become popular with the latest advancements in the networks and telecommunication technology.

Switching is relatively simple compared with the path determination. The concept of switching is like, a host determines like it should send some packet to another host. By some means it acquires the routers address and sends the packet addressed specifically to the routers MAC address, with the protocol address of the destination host. The router then examines the protocol address and verifies whether it know how to transfer the data to its destination. If it knows how to transfer the data then it forwards the packet to its destination and if it doesn't then it drops the packet. Routing is mainly classified into static routing and dynamic routing. Static routing refers to the routing strategy being stated manually or statically, in the router. Static routing maintains a routing table usually written by a networks administrator. The routing table doesn't depend on the state of the network status, i.e., whether the destination is active or not. Dynamic routing refers to the routing strategy that is being learnt by an interior or exterior routing protocol. This routing mainly depends on the state of the network i.e., the routing table is affected by the activeness of the destination. The major disadvantage with static routing is that if a new router is added or removed in the network then it is the responsibility of the administrator to make the necessary changes in the routing tables. But this is not the case with dynamic routing as each router announces its presence by flooding the information packet in the network so that every router within the network learn about the newly added or removed router and its entries. Similarly this is the same with the network segments in the dynamic routing.

Classification of Dynamic Routing Protocols

Dynamic routing protocols are classified depending on what the routers tell each other and how they use the information to form their routing tables. They are Distance vector protocols and Link state protocols Most of the protocols available in the networks fit into one of the two categories.

Distance Vector Protocols

By using the distance vector protocols, each router over the internetwork send the neighboring routers, the information about destination that it knows how to reach. Moreover to say the routers sends two pieces of information first, the router tells, how far it thinks the destination is and secondly, it tells in what direction (vector) to use to get to the destination. When the router receives the information from the others, it could then develop a table of destination addresses, distances and associated neighboring routers, and from this table then select the shortest route to the destination. Using a distance vector protocol, the router simply forwards the packet to the neighboring host (or destination) with the available shortest path in the routing table and assumes that the receiving router will know how to forward the packet beyond that point. The best example for this is the routing information protocol (RIP).

Link-State Protocols

In link state protocols, a router doesn't provide the information about the destination instead it provides the information about the topology of the network. This usually consist of the network segments and links that are attached to that particular router along with the state of the link i.e., whether the link is in active state or the inactive state. This information is flooded throughout the network and then every router in the network then builds its own picture of the current state of all the links in the network.

Mobile Ad-hoc Networks

An ad-hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any stand-alone infrastructure or centralized administration. Mobile Ad-hoc networks are self-organizing and self-configuring multihop wireless networks where, the structure of the network changes dynamically. This is mainly due to the mobility of the nodes. Nodes in these networks utilize the same random access wireless channel, cooperating in a friendly manner to engaging themselves in multihop forwarding. The nodes in the network not only acts as hosts but also as routers that route data to/from other nodes in network.

Classification of routing Protocols in MANET's

Classification of routing protocols in MANET's can be done in many ways, but most of these are done depending on routing strategy and network structure. According to the routing strategy the routing protocols can be categorized as Table-driven and source initiated, while depending on the network structure these are classified as flat routing, hierarchical routing and geographic position assisted routing. Both the Table-driven and source initiated protocols come under the Flat routing.

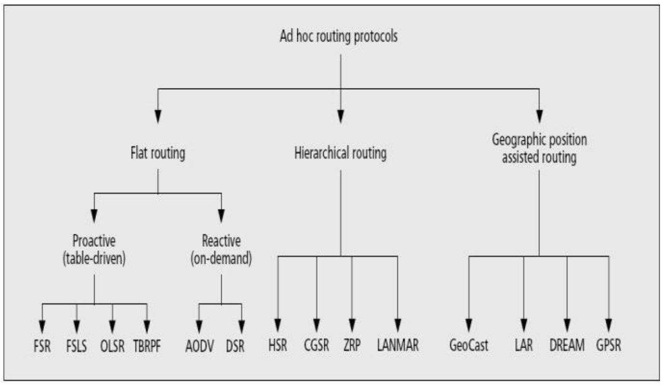

Figure: Classification of Routing Protocols In Mobile Ad-hoc Networks

Table-Driven routing protocols(Proactive) These protocols are also called as proactive protocols since they maintain the routing information even before it is needed. Each and every node in the network maintains routing information to every other node in the network. Routes information is generally kept in the routing tables and is periodically updated as the network topology changes. Many of these routing protocols come from the link-state routing. There exist some differences between the protocols that come under this category depending on the routing information being updated in each routing table. Furthermore, these routing protocols maintain different number of tables. The proactive protocols are not suitable for larger networks, as they need to maintain node entries for each and every node in the routing table of every node. This causes more overhead in the routing table leading to consumption of more bandwidth.

On Demand routing protocols(Reactive)

These protocols are also called reactive protocols since they don't maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The route discovery usually occurs by flooding the route request packets throughout the network.

Destination Sequenced Distance Vector (DSDV) Protocol

The destination sequenced distance vector routing protocol is a proactive routing protocol which is a modification of conventional Bellman-Ford routing algorithm. This protocol adds a new attribute, sequence number, to each route table entry at each node. Routing table is maintained at each node and with this table, node transmits the packets to other nodes in the network. This protocol was motivated for the use of data exchange along changing and arbitrary paths of interconnection which may not be close to any base station.

Protocol Overview and activities

Each node in the network maintains routing table for the transmission of the packets and also for the connectivity to different stations in the network. These stations list for all the available destinations, and the number of hops required to reach each destination in the routing table. The routing entry is tagged with a sequence number which is originated by the destination station. In order to maintain the consistency, each station transmits and updates its routing table periodically. The packets being broadcasted between stations indicate which stations are accessible and how many hops are required to reach that particular station. The packets may be transmitted containing the layer 2 or layer 3 address.
Number and the following information for each new route:
– The destination address
– The number of hops required to reach the destination and
– The new sequence number, originally stamped by destination

Advantages of DSDV

– DSDV protocol guarantees loop free paths.
– Count to infinity problem is reduced in DSDV.
– We can avoid extra traffic with incremental updates instead of full dump updates.
– Path Selection: DSDV maintains only the best path instead of maintaining multiple paths to every destination. With this, the amount of space in routing table is reduced.

Limitations of DSDV

– Wastage of bandwidth due to unnecessary advertising of routing information even if there is no change in the network topology.
– DSDV doesn’t support Multi path Routing.
– It is difficult to determine a time delay for the advertisement of routes [7].
– It is difficult to maintain the routing table’s advertisement for larger network. Each and every host in the network should maintain a routing table for advertising. But for larger network this would lead to overhead, which consumes more bandwidth.

Ad-hoc On-Demand Distance Vector (AODV) Protocol

AODV is a very simple, efficient, and effective routing protocol for Mobile Ad hoc Networks which do not have fixed topology. This algorithm was motivated by the limited bandwidth that is available in the media that are used for wireless communications.
It borrows most of the advantageous concepts from DSR and DSDV algorithms. The on demand route discovery and route maintenance from DSR and hop-by-hop routing, usage of node sequence numbers from DSDV make the algorithm cope up with topology and routing information. Obtaining the routes purely on-demand makes AODV a very useful and desired algorithm for MANETs.

Working of AODV

Each mobile host in the network acts as a specialized router and routes are obtained as needed, thus making the network self-starting. Each node in the network maintains a routing table with the routing information entries to it’s neighbouring nodes, and two separate counters: a node sequence number and a broadcast-id. When a node (say, source node ‘S’) has to communicate with another (say, destination node ‘D’), it increments its broadcast-id and initiates path discovery by broadcasting a route request packet RREQ to its neighbors. The RREQ contains the following fields: – source-addr

– source-sequence# - to maintain freshness info about the route to the source.
– dest-addr
– dest-sequence# - specifies how fresh a route to the destination must be before it is accepted by the source.
– hop-cnt

The (source-addr, broadcase-id) pair is used to identify the RREQ uniquely. Then the dynamic route table entry establishment begins at all the nodes in the network that are on the path from S to D.

As RREQ travels from node to node, it automatically sets up the reverse path from all these nodes back to the source. Each node that receives this packet records the address of the node from which it was received. This is called Reverse Path Setup. The nodes maintain this info for enough time for the RREQ to traverse the network and produce a reply to the sender and time depends on network size.

If an intermediate node has a route entry for the desired destination in its routing table, it compares the destination sequence number in its routing table with that in the

RREQ. If the destination sequence number in its routing table is less than that in the RREQ, it rebroadcasts the RREQ to its neighbors. Otherwise, it unicasts a route reply packet to its neighbor from which it was received the RREQ if the same request was not processed previously (this is identified using the broadcase-id and source-addr). Once the RREP is generated, it travels back to the source, based on the reverse path that it has set in it until traveled to this node. As the RREP travels back to source, each node along this path sets a forward pointer to the node from where it is receiving the RREP and records the latest destination sequence number to the request destination. This is called Forward Path Setup. If an intermediate node receives another RREP after propagating the first RREP towards source it checks for destination sequence number of new RREP. The intermediate node updates routing information and propagates new RREP only,

– If the Destination sequence number is greater, OR

– If the new sequence number is same and hop count is small, OR

Otherwise, it just skips the new RREP. This ensures that algorithm is loop-free and only the most effective route is used.

2. RELATED WORK

Routing protocols which researchers have developed to meet the challenges of WSN routing, many of which feature different methods of managing the issues associated with mobility. The two survey papers both find that every protocol identified also fit into the core categories of; reactive, proactive or hybrid routing protocols in additional to any other characteristics they exhibit.

A. Proactive Routing

Proactive protocols rely upon maintaining routing tables of known destinations, this reduces the amount of control traffic overhead that proactive routing generates because packets are forwarded immediately using known routes, however routing tables must be kept up-to-date; this uses memory and nodes periodically send update messages to neighbours, even when no traffic is present, wasting bandwidth.

B. Reactive Routing

Reactive Protocols use a route discovery process to flood the network with route query requests when a packet needs to be routed using source routing or distance vector routing. Source routing uses data packet headers containing routing information meaning nodes don't need routing tables; however this has high network overhead. Distance vector routing uses next hop and destination addresses to route packets, this requires nodes to store active routes information until no longer required or an active route timeout occurs, this prevents stale routes.

C. Hybrid Routing

Hybrid protocols combine features from both reactive and proactive routing protocols, typically attempting to exploit the reduced control traffic overhead from proactive systems whilst reducing the route discovery delays of reactive systems by maintaining some form of routing table. Survey papers successfully collect information from a wide range of literature and provide detailed and extensive reference material for attempting to deploy a WSN, both papers reach the conclusion that no single WSN routing protocol is best for every situation meaning analysis of the network and environmental requirements is essential for selecting an effective protocol.

3. EARLY WSN ROUTING PROTOCOLS

The next piece of literature is a protocol performance comparison by which compares the proactive Destination Sequenced Distance Vector (DSDV) protocol and the reactive Dynamic Source Routing (DSR) protocol; these protocols were developed in 1994 and were amongst the earliest MANET routing protocols identified using the previous survey papers.

A. Destination Sequenced Distance Vector (DSDV)

The proactive DSDV protocol was proposed by and is based upon the Bellman-Ford algorithm to calculate the shortest number of hops to the destination. Each DSDV node maintains a routing table which stores; destinations, next hop addresses and number of hops as well as sequence numbers; routing table updates are sent periodically as incremental dumps limited to a size of 1 packet containing only new information. DSDV compensates for mobility using sequence numbers and routing table updates, if a route update with a higher sequence number is received it will replace the existing route thereby reducing the chance of routing loops, when a major topology change is detected a full routing table dump will be performed, this can add significant overhead to the network in dynamic scenarios.

B. Dynamic Source Routing (DSR)

The reactive DSR Protocol is broken into two stages; route discovery phase and route maintenance phase, these phases are triggered on demand when a packet needs routing. Route discovery phase floods the network with route requests if a suitable route is not available in the route. DSR uses a source routing strategy to generate a complete route to the destination, this will then be stored temporarily in nodes route cache. DSR addresses mobility issues through the use of packet acknowledgements; failure to receive an acknowledgement causes packets to be buffered and route error messages to be sent to all upstream nodes. Route error messages trigger the route maintenance phase which removes incorrect routes from the route cache and undertakes a new route discovery phase.

C. Mobility Models

Reference [10] compares the performance of DSR and DSDV using simulations against 4 different mobility models; these are mathematic models which control the motion of nodes around the simulation; this allows researchers to measure the effect of mobility upon the routing protocols performance. Various mobility models are used to simulate different situations such as high speed vehicular networks or lower mobility ad-hoc conference users, however reveals that many studies perform protocol evaluation almost exclusively using the random waypoint mobility model. This research is supported by findings who claim that the random waypoint model is the most widely used mobility model, however discrepancies were identified between the models behaviour and real world scenarios where users typically move in groups, due to this the model may not be appropriate for exclusive testing.

This protocol is based on the location information of senor nodes in the wireless sensor networks. It assumes that each node would know its own location and a neighbor sensor node's location before sensor nodes sensing and collect the peripheral information. The distance between neighboring sensor nodes can be computed on the basis of the incoming signal strength. In this project, to obtain the transmission paths for emergency messages, consider the structural similarities between the spider-webs and road segments, and try to create a spider web-like model for WSNs.

4. PROPOSED SYSTEM

We propose E-STAR for establishing stable and reliable routes in heterogeneous multihop wireless networks. E-STAR combines payment and trust systems with a trust-based and energy-aware routing protocol. The payment system rewards the nodes that relay others' packets and charges those that send packets. The trust system evaluates the nodes' competence and reliability in relaying packets in terms of multi-dimensional trust values. The trust values are attached to the nodes' public-key certificates to be used in making routing decisions. We develop two routing protocols to direct traffic through those highly-trusted nodes having sufficient energy to minimize the probability of breaking the route. By this way, E-STAR can stimulate the nodes not only to relay packets, but also to maintain route stability and report correct battery energy capability.

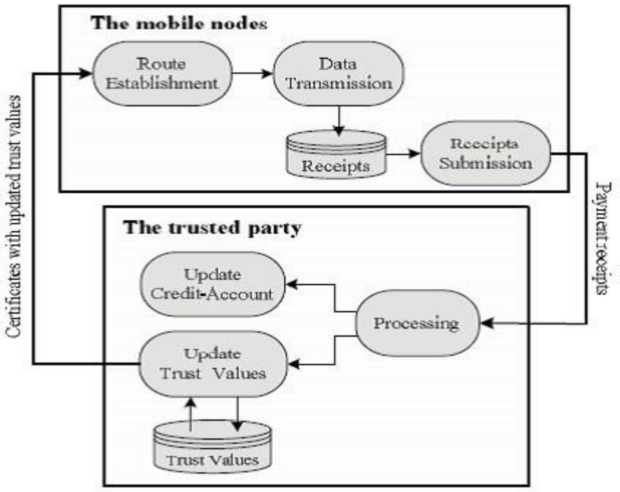

Fig shows that E-STAR has three main phases. In Data Transmission phase, the source node sends messages to the destination node. In Update Credit-Account and Trust Values phases, TP determines the charges and rewards of the nodes and updates the nodes' trust values. Finally, in Route Establishment phase, trust-based and energy-aware routing protocol establishes stable communication routes.

Data Transmission Phase
Let the source node NS send messages to the destination node ND through a route with the intermediate nodes □X, □Y, and □Z. The route is established by the routing protocols, for the ith data packet, □S computes the signature CS(i) = {H(H(mi), ts, R, i)}KS+ and sends the packet <R, ts, i, mi, CS(i)> to the first node in the route. R, ts, and mi are the concatenation of the identities of the nodes in the route (R = IDS, IDX, IDY, IDZ, IDD), the route establishment time stamp, and the ith message, respectively. H(d) is the hash value resulted from hashing the data d using the hash function H(). {d}KS+ is the signature of d with the private key of CS. The purpose of the source node's signature is to ensure the message's authenticity and integrity and secure the payment by enabling TP to ensure that CS has sent i messages. Each intermediate node verifies CS(i) and stores CS(i) and H(mi) for composing the receipt. It also removes the previous ones (CS(i-1) and H(mi-1)) because CS(i) is

enough to prove transmitting i messages. Signing H(mi) instead of mi can reduce the receipt size because the smaller-size H(mi) is attached to the receipt instead of mi. The destination node generates a one-way hash chain by iteratively hashing a random value hS S times to obtain the hash chain {hS, hS-1,..., h1, h0}, where hi-1= H(hi) for 1 < i < S and h0 is called the root of the hash chain. The node signs h0 and R to authenticate the hash chain and links it to the route, and sends the signature to the source node in route establishment phase. In order to acknowledge receiving the message mi, the destination node sends ACK packet containing the preimage of the last released hash chain element or hi. Each intermediate node verifies the hash chain element by making sure that hi-1 is obtained from hashing hi, and saves hi for composing the receipt and removes hi- 1. The underlying idea is that CS(i) and hi are undeniable proofs for sending and receiving i messages, respectively. Each node in the route composes a receipt and submits it when it has a connection to TP to claim the payment and update its trust values. A receipt is a proof for participating in a route and sending, relaying, or receiving a number of messages. A receipt contains R, ts, i, H(mi), h0, hi, Cm, and an undeniable cryptographic token for preventing payment manipulation. Cm is data that depends on the used routing protocol, such as the number of messages the intermediate nodes commit to relay. The cryptographic token contains the hash value of the last source node's signature and Auth_Code. Auth_Code is the authentication code that authenticates the hash chain and the intermediate nodes to hold them accountable for breaking the route. Considering trust in routing decisions is essential in HMWN that is characterized by uncertainty in the nodes' behavior because they are autonomous and self-interested. A trust relationship is never absolute, but it is context dependent in the sense that a node's trust value depicts its ability to perform a specific action. For example, Alice may trust Bob to repair her computer but she may not trust Bob to repair her car. Trust is also dynamic or time-sensitive, so TP has to periodically evaluate the nodes' trustworthiness.

5. CONCLUSION

We have proposed E-STAR that uses payment/trust systems with trust-based and energy-aware routing protocol to establish stable/reliable routes in HMWNs. E-STAR stimulates the nodes not only to relay others' packets but also to maintain the route stability. It also punishes the nodes that report incorrect energy capability by decreasing their chance to be selected by the routing protocol. We have proposed routing protocols and evaluated them in terms of overhead and route stability. Our protocols can make informed routing decisions by considering multiple factors, including the route length, the route reliability based on the nodes' past behavior, and the route lifetime based on the nodes' energy capability. SRR establishes routes that can meet source nodes' trust/energy requirements. It is useful in establishing routes that avoid the low-trust nodes, e.g., malicious nodes, with low overhead. For BAR, destination nodes establish the most reliable routes but with more overhead comparing to SRR. The analytical results have demonstrated that E-STAR can secure the payment and trust calculation without false accusations. Moreover, the simulation results have demonstrated that E-STAR can improve the packet delivery ratio due to establishing stable routes.

6. REFERENCES

1. Y. Hu, M. Dong, K. Ota, et al. "Mobile Target Detection in Wireless Sensor Networks with Adjustable Sensing Frequency,"IEEE System Journal, Doi: 10.1109/JSYST.2014.2308391, 2014.

2. M. Dong, K. Ota, A. Liu, et al. "Joint Optimization of Lifetime and Transport Delay under Reliability Constraint Wireless Sensor Networks," IEEETransactions on Parallel and Distributed Systems, vol. 27, no. 1, pp. 225-236, 2016.

3. S. He, J. Chen, F. Jiang, et al. "Energy provisioning in wireless rechargeable sensor networks," IEEE transactions on mobile computing, vol. 12, no. 10, pp. 1931-1942, 2013.

4. X.Liu,M. Dong, K. Ota, P. Hung, A. Liu. "Service Pricing Decision in Cyber-Physical Systems: Insights from Game Theory," IEEE Transactions on Services Computing,vol. 9, no. 2, pp. 186-198, 2016.

5. C. Zhu, H. Nicanfar, V. C. M. Leung, et al. "An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration," IEEE Transactions on Information Forensics and Security, vol. 10, no. 1, pp. 118-131, 2015.

6. A.Liu, M.Dong, K.Ota, et al."PHACK：An Efficient Scheme for Selective Forwarding Attack Detecting in WSNs," Sensors, vol. 15, no. 12, pp. 30942-30963, 2015.

7. A. Liu, X. Jin, G.Cui, Z. Chen, "Deployment guidelines for achieving maximum lifetime and avoiding energy holes in sensor network,"Information Sciences,vol. 230, pp.197-226, 2013.

8. Z. Zheng, A. Liu, L. Cai, et al."Energy and Memory Efficient Clone Detection in Wireless Sensor Networks,"IEEE Transactions on Mobile Computing.vol. 15, no. 5, pp.1130-1143,2016.

9. T. Shu, M. Krunz,S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 941-954, 2010.

10. P. Zhou, S. Jiang, A. Irissappane, et al. "Toward Energy-Efficient Trust System Through Watchdog Optimization for WSNs," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 613-625, 2015.

11. S. Shen, H. Li, R. Han, et al. "Differential game-based strategies for preventing malware propagation in wireless sensor networks," IEEE Transactions on Information Forensics and Security, vol.9, no. 11, pp. 1962-1973, 2014.

12. O. Souihli, M.Frikha, B.H.Mahmoud, "Load-balancing in MANET shortest-path routing protocols," Ad Hoc Networks, vol. 7, no. 2, pp. 431-442, 2009.

13. J. Long, A. Liu, M. Dong, et al. "Anenergy-efficient and sink-location privacy enhanced scheme for WSNs through ring based routing," Journal of Parallel and Distributed Computing, vol. 81, pp. 47-65, 2015.

14. S. He, J. Chen, X. Li, et al. "Mobility and intruder prior information improving the barrier coverage of sparse sensor networks," IEEE transactions on mobile computing, vol. 13, no. 6, pp.1268-1282, 2015.

15. S. H. Seo, J. Won, S. Sultana, et al. "Effective key management in dynamic wireless sensor networks," IEEE Transactions on Information Forensics and Security, vol. 10, no. 2, pp. 371-383, 2014.