Optimized and Energy Efficient Data Dissemination Technique for D2D Communication in Wireless Networks

S.Abirami, M.Divya,G.Divyapriyanka, U.Naveena,

Final CSE

I.Vallirathi, Assistant Professor/CSE

PET Engineering College

Abstract

In wireless sensor networks, this exhaustion of energy will be more due to its infrastructure less nature and mobility. This may lead a node to drain their energy and also affect the performance of routing protocol and network lifetime. Several researches have gone so far for predicting node lifetime and link lifetime. To address this problem a new algorithm has been developed which utilizes the network parameters relating to dynamic nature of nodes viz. energy drain rate, relative mobility estimation to predict the route lifetime. But this has given a problem of network congestion and delay. To mitigate this problem in this paper, we proposed a particle swarm optimization based routing (PSOR). PSOR algorithm is designed to maximize the lifetime of WSNs. The algorithm uses a good strategy considering energy levels of the nodes and the lengths of the routed paths. In this paper, we have compared the performance results of our PSOR approach to the results of the Genetic algorithm. Various differently sized networks are considered, and our approach gives better results than Genetic algorithm in terms of energy consumption. The main goal of our study was to maintain network life time at a maximum, while discovering the shortest paths from the source nodes to the base node using a particle swarm based optimization technique called PSO.Particle Swarm Optimization based Routing protocol (PSOR) where we have taken energy efficiency as major criteria for performing routing and deriving optimized path for data forwarding and processing to base node. The PSOR generates a whole new path of routing by taking energy as fitness value to judge different path and choose best optimized path whose energy consumption is less as compared to other routing paths.

Keywords: Particle Swarm Optimization based Routing protocol, Genetic algorithm, Ad Hoc Networks

CHAPTER 1

INTRODUCTION

WSN consists of many mobile nodes that can communicate directly with each other or through intermediate nodes. Often, nodes in a WSN operate with batteries and can roam freely, and thus, a node may exhaust its energy or move away without giving any notice to its cooperative nodes. This will cause the changes in network topology. The development of an efficient routing protocol that can provide high-quality communications among mobile hosts, this is one of the important and challenging problems in the design of ad hoc networks. Several studies on the dynamic nature of WSNs have been done. These studies often attempt to find a stable route which has a long lifetime. We can classify these solutions into two main groups:

node lifetime routing algorithms and link lifetime routing algorithms.

Node lifetime routing algorithm depends upon the energy state of nodes, such as residual energy and energy drain rate, this routing algorithms often select a path c In WSN nodes may communicate through intermediate nodes. Due to mobility, the changes in the network topology will be more. One of the important and challenging problems in the design of ad hoc networks is to develop an efficient routing protocol. Several studies on the dynamic nature of WSNs have been done. In WSNs, a route consists of multiple links in series, and thus, its lifetime depends on the lifetime of each node, as well as the wireless links between adjacent nodes. The main contribution of this paper is that we combine node lifetime and link lifetime in our route lifetime -prediction algorithm, which explores the dynamic nature of mobile nodes such as the energy drain rate of nodes and the relative mobility estimation rate at which adjacent nodes move apart in a route-discovery period that predicts the lifetime of routes that are discovered, and then, we select the longest lifetime route for data forwarding when making a route decision.

Cross-layer is becoming an important studying area for wireless communications. In addition, the traditional layered approach presents three main problems:

1. Traditional layered approach cannot share different information among different layers which leads to each layer not having complete information. The traditional layered approach cannot guarantee the optimization of the entire network.
2. The traditional layered approach does not have the ability to adapt to the environmental change.
3. Because of the interference between the different users, access confliction, fading, and the change of environment in the wireless sensor networks, traditional layered approach for wired networks is not applicable to wireless networks.

In many surveillance applications of WSN s, tracking a mobile target (e.g., a human being or a vehicle) is one of the main objectives. Unlike detection that studies discrete detection events a target tracking system is often required to ensure continuous monitoring, i.e., there always exist nodes that can detect the target along its trajectory (e.g., with low detection delay or high coverage level). Therefore, the most stringent criterion of target tracking is to track with zero detection delay or 100% coverage. Wireless sensor networks (WSN s) are widely applied in monitoring, sensing, and collecting the information of interest in the environment. Localization of target nodes is a fundamental problem in wireless sensor networks. Up to now, the most existing localization algorithms of WSNs can be classified into two categories: range-based and range-free. Range-based algorithms use distance or angle estimates in their location estimations. Range-free algorithms use connectivity information between unknown nodes and anchor nodes. Range-based localization algorithms need to measure the actual distances or orientation between adjacent nodes, and then use the measured data to locate unknown nodes. There

will be measurement errors in practical localization systems that result in noisy range estimations. Thus, accuracy in the position estimation phase is highly sensitive to range measurements. Without improving range estimation or adding some other information related to localization, the accuracy of the current range-based algorithms cannot be improved obviously.

Indoor localization of WSNs has been a hot research topic for the last several years. Due to the randomness of targets moving and the complicated indoor environment, it is very different to locate indoor mobile target.

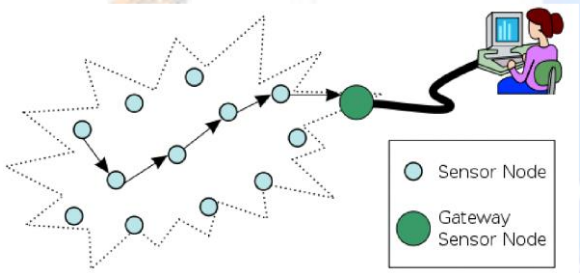

Fig 1.1wireless sensor networks

Challenges

Although WSNs have some simplifications in design, we have some issues that affects the feasibility and performance of WSNs. Most important ones are, namely:

• Limited and variable wireless transmission range.

• Broadcast nature of the wireless medium.

• Packet losses due to transmission errors.

• No centralized administration or standard support services.

• Route changes because of the dynamic structure of WSNs (mobility) which may cause to loss of packets

• Nodes with limited power

• Potential network partitions due to mobility and structure of wireless medium

• Security issues

Usage Scenarios and Scalability of Ad Hoc Networks

Ad hoc networks may have different usage scenarios. In [2], it is divided into 4 subcategories:

- Enterprise networks
- Hot spot networks
- Community networks
- Home/Apartment networks

But, also we know that it is used in military environments, emergency operations, meeting (e.g. conference) halls, etc. This information is important, because each of these scenarios has specific values for some parameters existing in every ad hoc network, and these parameters affect the usage, performance and feasibility of ad hoc networks very dramatically.

For ex. number of nodes is very different in a home network and an enterprise network, or mobility of nodes is definitely different in military environment and hot spot networks, etc.

Also, the consideration for each scenario varies. For ex. in a home network, throughput of the network could be the most important metric, while security is vital for military environment networks.

One very important issue in ad hoc networking is the scalability. While scalability of an ad hoc network algorithm/method can be measured in a variety of ways, we can define it as the efficiency of the algorithm/method as the parameter converges to infinity (or more realistically, the maximum value for that parameter that can be seen). Scalability is a great tool for efficiency

measurement of a method or an algorithm for ad hoc networks. So, any proposed method/algorithm should be scalable according to above parameters, especially for independent parameters. Because, independent parameters can change independently from any other parameter, at very unpredicted levels.

According to above definitions and classifications, we can see that scalability of an algorithm/method can be optimized by considering the network's usage area. Since, it is not impossible to make an ad hoc network algorithm/method (e.g. routing protocol), one can predict the upper and lower bounds for the parameters at the usage context and design his algorithm accordingly.

CHAPTER 2
LITERATURE REVIEW

1) Title: An intelligent SDN framework for 5G heterogeneous networks

Author name: S. Sun, L. Gong, B. Rong, and K. Lu,

This article proposes a software defined network (SDN) based intelligent model that can efficiently manage the heterogeneous infrastructure and resources. In particular, we first review the latest SDN standards and discuss the possible extensions. We then discuss the advantages of SDN in meeting the dynamic nature of services and requirements in 5G HetNets. Finally, we develop a variety of schemes to improve traffic control, subscriber management, and resource allocation. Performance analysis shows that our proposed system is reliable, scalable, and implementable.

2) Title: EPPDR: An Efficient Privacy-Preserving Demand Response Scheme with Adaptive Key Evolution in Smart Grid .

Author name: H. Li, X. Lin, H. Yang, X. Liang, R. Lu, and X. Shen

In this paper, we propose an efficient privacy-preserving demand response (EPPDR) scheme which employs a homomorphic encryption to achieve privacy-preserving demand aggregation and efficient response. In addition, an adaptive key evolution technique is further investigated to ensure the users' session keys to be forward secure. Security analysis indicates that EPPDR can achieve privacy-preservation of electricity demand, forward secrecy of users' session keys, and evolution of users' private keys. In comparison with an existing scheme which also achieves forward secrecy, EPPDR has better efficiency in terms of computation and communication overheads and can adaptively control the key evolution to balance the trade-off between the communication efficiency and security level.

3) Title: Tennison: A distributed SDN framework for scalable network securityL.

Author name: L. Fawcett.S. Scott-Hayward, M. Broadbent, A. Wright, and N. Race,

SDN's global view provides a means of monitoring and defense across the entire network. However, current SDN-based security systems are limited by a centralized framework that introduces significant control plane overhead, leading to the saturation of vital control links. In this paper, we introduce TENNISON, a novel distributed SDN security framework that combines the efficiency of SDN control and monitoring with

the resilience and scalability of a distributed system. TENNISON offers effective and proportionate monitoring and remediation, compatibility with widely available networking hardware, support for legacy networks, and a modular and extensible distributed design. We demonstrate the effectiveness and capabilities of the TENNISON framework through the use of four attack scenarios. These highlight multiple levels of monitoring, rapid detection, and remediation, and provide a unique insight into the impact of multiple controllers on network attack detection at scale.

4) Title: Smart wireless sensor network management based on software-defined networking.

Author name: A.DeGante, M.Aslan, andA.Matrawy,

In this position paper, we propose the use of software-defined networking (SDN) in wireless sensor networks (WSNs) for smart management. We argue that smart management using SDN promises a solution to some of inherent problems in WSN management. Furthermore, we propose a generic architecture for a base station in a software-defined wireless sensor network. We also propose a general framework for a software-defined wireless sensor network where the controller is implemented at the base station. We then raise some important questions that need to be investigated in future research in software-defined wireless sensor networks.

5) Title: "Security in software-defined wireless sensor networks: Threats, challenges and potential solutions .

Author name: S. W. Pritchard, G. P. Hancke, and A. M. Abu-Mahfouz,

In this paper, we study the new security challenges of the control channel of SDMNs and propose a novel secure control channel architecture based on Host Identity Protocol (HIP). IPsec tunneling and security gateways are widely used in today's mobile networks. The proposed architecture utilized these technologies to protect the control channel of SDMNs. We implement the proposed architecture in a testbed and analyze the security features. Moreover, we measure the performance penalty of security of proposed architecture and analyze its ability to protect the control channel from various IP (Internet Protocol) based attacks.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 EXISTING SYSTEM

1) The relay-aided D2D communication underlaying the cellular network model is proposed and analyzed. Focusing on improving the energy efficiency of D2D links, we derive an optimal energy efficiency formulation under the constraints of power and quality of service (QoS). The optimization problem is a mixed integer nonlinear programming (MINLP) problem which is difficult to solve directly. Hence, we divided it into two sub problems, power allocation and relay selection.

2) Since the power allocation is a non-convex problem, we transform it into an equivalent subtractive form by employing the Dinkelbach

method, which is solved through the use of Lagrange dual decomposition.

3) Regarding the D2D pairs as agents, we propose a novel relay selection scheme based on Q-learning and limit the number of relays based on the placement to reduce the computation complexity.

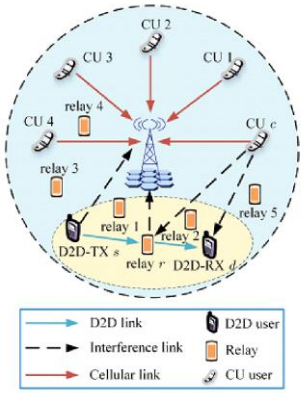

Fig : 3.1 System model for relay-aided D2D communication

4) At last, we evaluate the proposed joint power allocation and relay selection (JPARS) scheme through extensive simulations. The simulation results show that the proposed scheme achieves a higher energy efficiency of all D2D pairs than other such schemes.

3.1.1DRAWBACKS:

- It still requires much work to improve security and to investigate other transaction procedures.
- Furthermore, we have not yet grasped all issues which will arise in practical usage. Therefore, experiments in real networks will be indispensable.

3.2 PROPOSED SYSTEM:

In wireless sensor networks, this exhaustion of energy will be more due to its infrastructure less nature and mobility. This may lead a node to drain their energy and also affect the performance of routing protocol and network lifetime. Several researches have gone so far for predicting node lifetime and link lifetime. To address this problem a new algorithm has been developed which utilizes the network parameters relating to dynamic nature of nodes viz. energy drain rate, relative mobility estimation to predict the route lifetime. But this has given a problem of network congestion and delay.

To mitigate this problem in this project, we proposed a particle swarm optimization based routing (PSOR). PSOR algorithm is designed to maximize the lifetime of WSNs. The algorithm uses a good strategy considering energy levels of the nodes and the lengths of the routed paths. In this paper, we have compared the performance results of our PSOR approach to the results of the Genetic algorithm. Various differently sized networks are considered, and our approach gives better results than Genetic algorithm in terms of energy consumption. The main goal of our study was to maintain network life time at a maximum, while discovering the shortest paths from the source nodes to the base node using a particle swarm based optimization technique called PSO.

Particle Swarm Optimization based Routing protocol (PSOR) where we have taken energy efficiency as major criteria for performing routing and deriving optimized path for data forwarding and processing to base node. The PSOR generates a whole new path of routing by taking energy as fitness value to judge different path and choose best optimized path whose energy consumption is less as compared to other routing paths.

In WSN, a route consists of multiple links in series. A link is nothing but connection between two adjacent nodes which have limited battery energy and can roam freely. Link breaks occur due to lack of energy or nodes moving away out of each other's transmission range. Link lifetime depends on lifetime of node and lifetime of connection. In this paper we just combine both the lifetimes using route lifetime prediction algorithm which explores the dynamic nature then select the least dynamic route for persistent data forwarding. But this has given a problem of network congestion and delay. To mitigate this problem, in this paper we have implemented an algorithm which uses the prediction parameters that are and fuzzy rules have been formed to decide on the node status. This status information is made to exchange among all the nodes. Before every transmission the status of each and every node is verified. Even for a weak node, the performance of a route recovery mechanism is made in such a way that corresponding routes are diverted to the strong nodes. Thereby it reduces the data loss and communication overhead using PSO prediction algorithm.

PSO is an optimization technique developed and is inspired by the social behavior of bird flock. Input to the PSO algorithm is given in the form of particles, hence in the case of networks, the multiple paths (between two nodes) obtained is encoded as particles. Here we use a modified version of Indirect Encoding Technique. Particles (or sequence of nodes or path) obtained by indirect encoding scheme, serve as input to the PSO algorithm. Here, our objective is to find the particle which has the maximum cost (bandwidth), associated with the links of the particle (or path). In the formulae for velocity and position have been specified. The particle's best position is referred to as pBest and the best position in comparison to all other particles is referred to as gBest, i.e. the global best. In every iteration, the p Best is calculated, using which we obtain the gBest value, which is the shortest path of the network. The pBest value is calculated depending on the value of fitness of each particle in every iteration. The fitness value depends upon the bandwidth associated with the particles. The fitness value is calculated .

3.2.1AD HOC ON-DEMAND DISTANCE VECTOR (AODV)

AODV is essentially a combination of both DSR and DSDV. It borrows the basic on-demand mechanism of Route Discovery and Route Maintenance from DSR, plus the use of hop-by-hop routing, sequence numbers, and periodic beacons from DSDV.

Basic Mechanisms

When a node S needs a route to some destination D, it broadcasts a ROUTE REQUEST message to its neighbors, including the last known sequence number for that destination. The ROUTE REQUEST is flooded in a controlled manner through the network until it reaches a node that has a route to the destination. Each node that forwards the ROUTE REQUEST creates a reverse route for itself back to node S. When the ROUTE REQUEST reaches a node with a route to D, that node generates a ROUTE REPL Y that contains the number of hops necessary to reach D and the sequence number for D most recently seen by the

node generating the REPLY. Each node that participates in forwarding this REPLY back toward the originator of the ROUTE REQUEST (node S), creates a forward route to D. The state created in each node along the path from S to D is hop-by-hop state; that is, each node remembers only the next hop and not the entire route, as would be done in source routing.

In order to maintain routes, AODV normally requires that each= node periodically transmit a HELLO message, with a default rate of once per second. Failure to receive three consecutive HELLO messages from a neighbor is taken as an indication that the link to the neighbor in question is down. Alternatively, the AODV specification briefly suggests that a node may use physical layer or link layer methods to detect link breakages to nodes that it considers neighbors. When a link goes down, any upstream node that has recently forwarded packets to a destination using that link is notified via an UNSOLICITED ROUTE REPL Y containing an infinite metric for that destination. Upon receipt of such a ROUTE REPL Y, a node must acquire a new route to the destination using Route Discovery as described above.

Implementation Decisions

We initially implemented AODV using periodic HELLO messages for link breakage detection as described in the AODV specification. For comparison, we also implemented a version of AODV that we call AODV -LL (link layer), instead using only link layer feedback from 802.11 as in DSR, completely eliminating the standard AODV HELLO mechanism. Such an approach saves the overhead of the periodic HELLO messages, but does somewhat change the fundamental nature of the protocol; for example, all link breakage detection in AODV –LL is only on-demand, and thus a broken link cannot be detected until a packet needs to be sent over the link, whereas the periodic HELLO messages in standard AODV may allow broken links to be detected before a packet must be forwarded. Nevertheless, we found our alternate version AODV -LL to perform significantly better than standard AODV, and so we report measurements from that version here.

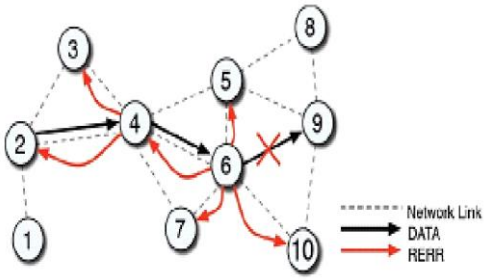

Fig 3.3.2 Route Maintanance

In addition, we also changed our AODV implementation to use a shorter timeout of 6 seconds before retrying a ROUTE REQUEST for which no ROUTE REPL Y has been received (RREP W AIT TIME). The value given in the AODV specification was 120 seconds, based on the other constants specified there for AODV. However, a ROUTE REPL Y can only be returned if each node along the discovered route still has a reverse route along which to return it, saved from when the ROUTE REQUEST was propagated. Since the specified timeout for this reverse route information in each node is only 3 seconds, the original ROUTE REPL Y timeout value of 120 seconds unnecessarily limited the protocol's ability to recover from a dropped ROUTE REQUEST or ROUTE REPLY packet

ADVANTAGES:

- Maximizing the lifetime of the sensor nodes, it is preferable to distribute the energy dissipated throughout the wireless sensor network in order to minimize maintenance and maximize overall system performance while routing.
- Energy efficient routing across the network.
- Consumption of sensor energy is less.
- Best routing path with least distance.

CHAPTER 4
EXPERIMENTAL RESULT AND DISCUSSION

This study used ns-2 as the network simulator and conducted numerous simulations to evaluate the PSO performance. All sensor nodes are randomly scattered with a uniform distribution. Randomly select one of the deployed nodes as the source node. The location of the sink is randomly determined. This study evaluates the routing performance under scenarios with different numbers of sensor nodes.

In this section we discuss about simulation results of this proposed PSO frame work. Discuss the process using simulation output screen shots from NS2 simulation tool. Mention all the process one by one and give explanation for all screen shots.

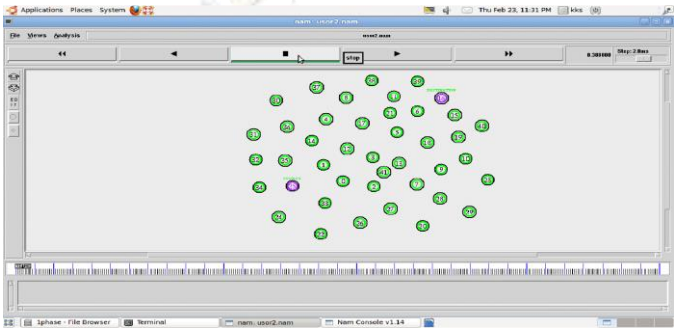

Fig 4.1Node initialization

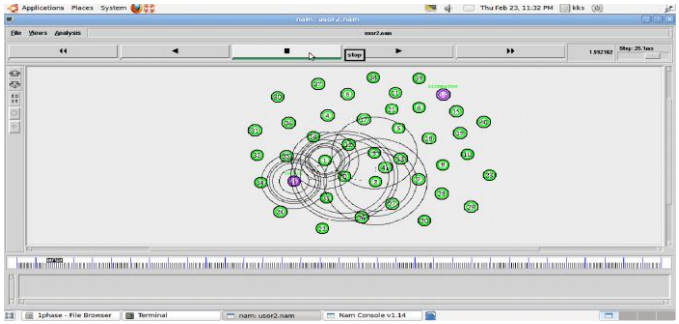

Fig 4.2 Sending hello packets to neighbor nodes

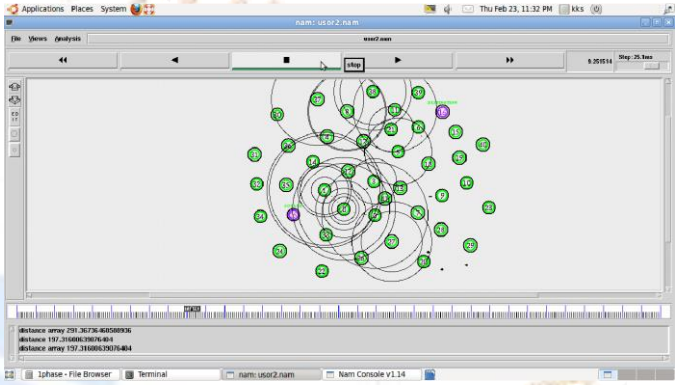

Fig 4.3 Checking distance of neighbor nodes

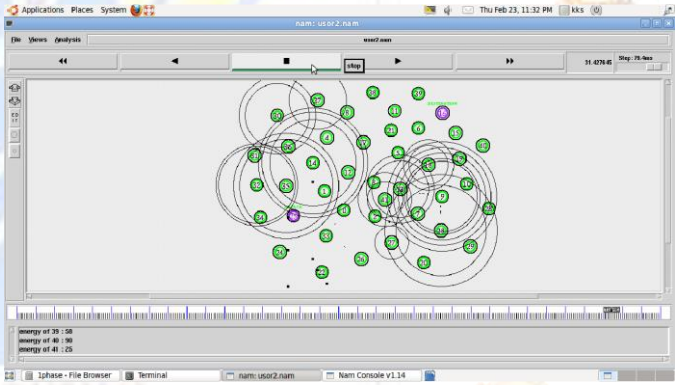

Fig 4.4 Calculating energy of nodes

This study evaluates the following main performance metrics:

Distance Table

In this process sending hello packets for all nodes initially to calculate and define the distance of all nodes from each neighbors, here consider each node as a source node and all source nodes having neighbor nodes in network it calculate

distance from source node to each neighbor nodes, using distance calculation formulas.

CHAPTER 5

CONCLUSION

we proposed a particle swarm optimization based routing (PSOR). PSOR algorithm is designed to maximize the lifetime of WSNs. The algorithm uses a good strategy considering energy levels of the nodes and the lengths of the routed paths

Particle Swarm Optimization based Routing protocol (PSOR) where we have taken energy efficiency as major criteria for performing routing and deriving optimized path for data forwarding and processing to base node. The PSOR generates a whole new path of routing by taking energy as fitness value to judge different path and choose best optimized path whose energy consumption is less as compared to other routing paths. Even for a weak node, the performance of a route recovery mechanism is made in such a way that corresponding routes are diverted to the strong nodes. The concept of this model is based on the fact is greater the distance travelled to send data more is the consumption of sensor energy. The algorithm is done by using concept of PSO. Our results prove that after a considerable optimum path can be calculated using PSO which shows better result than GA giving us best r outing path with least distance to be travelled. Thereby it reduces the data loss and communication overhead using PSO prediction algorithm. Simulation results show that the PSO protocol outperforms the other protocols thereby this protocol reducing congestion delay and increasing network lifetime.

REFERENCES

- H. Li, X. Lin, H. Yang, X. Liang, R. Lu, and X. Shen, "EPPDR: An Efficient Privacy-Preserving Demand Response Scheme with Adaptive Key Evolution in Smart Grid," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no.8, pp. 2053-2064, 2014.
- S. Sun, L. Gong, B. Rong, and K. Lu, "An intelligent SDN framework for 5G heterogeneous networks," IEEE Commun. Mag., vol. 53, no. 11, pp. 142–147, Nov. 2015.
- L. Fawcett, S. Scott-Hayward, M. Broadbent, A. Wright, and N. Race, "Tennison: A distributed SDN framework for scalable network security," IEEE J. Sel. Areas Commun., vol. 36, no. 12, pp. 2805–2818, Dec. 2018.
- A.DeGante,M.Aslan,andA.Matrawy, "Smart wireless sensor network management based on software-defined networking," inProc. IEEE Commun. Biennial Symp., Jun. 2014, pp. 71–75.
- S. W. Pritchard, G. P. Hancke, and A. M. Abu-Mahfouz, "Security in software-defined wireless sensor networks: Threats, challenges and potential solutions," in Proc. IEEE 15th Int. Conf. Ind. Informat. (INDIN), Jul. 2017, pp. 168–173
- C. Habib, A. Makhoul, R. Darazi, and C. Salim, "Self-adaptive data collection and fusion for health monitoring based on body sensor networks,"IEEE Trans. Ind. Informat., vol. 12, no. 6, pp. 2342–2352, Dec. 2016.