IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

Performance Improvement of a Secure Mechanism for Big Data Collection in Large Scale Internet of Vehicle Using MATLAB

E.Juliet Priscilla[1] Prof. Dr.K.Mathan[2]

Student, Department of EEE, Hindusthan College of Engineering and Technology, Coimbatore[1]

Assistant Professor, Department of EEE, Hindusthan College of Engineering and Technology, Coimbatore[2]

Abstract: VANETs (Vehicular Ad-hoc Network) are characterized by a very dynamic topology with partial infrastructure support, patterned mobility, and mobile nodes with sufficient amount of resources, intermittent connectivity and varied channel behavior. For this purpose, we always use the location information that vehicles share among them through repetitive messages that are transmitted in the VANET system. This paper proposes a methodical approach to improve the Quality of Service (QoS) evaluation in wireless and mobile networks. In this proposed framework, we used novel schemes for secure transmission and big data collection in Vehicular Ad hoc Networks. Secure information collection scheme for big data in large scale IoV. Single sign-on algorithm for authentication are utilized with improved efficiency. The proposed secure data exchange algorithm using message digest and random key contributes to overhead reduction. The business data is transferred in plain text form while the confidential data is transferred in cipher text form. The collected big data will be processed using hadoop architecture to achieve the unified management. In experimental results the proposed secure information collection scheme achieves high efficiency and security for big data in large scale IoV.

Keywords: Vehicular ad-hoc network, Quality of Service, Security Mechanism, Big Data Collection.

I. INTRODUCTION

Vehicular ad hoc networks (VANETs) have recently been proposed as one of the promising ad hoc networking techniques that can provide both drivers and passengers with a safe and enjoyable driving experience. VANETs can be used for many applications with vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. In the United States, motor vehicle traffic crashes are the leading cause of death for all motorists between two and thirty-four years of age. In 2009, the National Highway Traffic Safety Administration (NHTSA) reported that 33,808 people were killed in motor vehicle traffic crashes. The US Department of Transportation (US-DOT).

Estimates that over half of all congestion events are caused by highway incidents rather than by rush-hour traffic in big cities. [1] The US-DOT also notes that in a single year, congested highways due to traffic incidents cost over $75 billion in lost worker productivity and over 8.4 billion gallons of fuel. Some of the significant applications of VANETs are road safety applications including collision and other safety warning systems, driver convenience and information systems, and, in the future, intelligent traffic management systems.

The convergence of technology encompasses information communications, environmental protection, energy conservation, and safety.
To succeed in this emerging market, acquisition of core technologies and standards will be crucial to securing a strategic advantage. However, the integration of the IoV [2] with other infrastructures should be as important as the building of the IoV technologies themselves. As a consequence of this, the IoV [3] will become an integral part of the largest Internet of Things (IoT) infrastructure by its completion. Here, it must be emphasized as primary, that collaboration and interconnection between the transportation sector and other sectors (such as energy, health-care, environment, manufacturing, and agriculture, etc...) [4] Will be the next step in IoV development.

Nowadays, there existed some related works which focus on security of big data and IoV. In proposed a security scheme of data messages exchanged between users and RSUs, but the scalability of IoV is still a remained problem to solve. [9][10] The authors in work at the big data area and developed the security and privacy mechanisms. As an important technology in big data area, the security of Hadoop is also addressed in. Liu et al. proposed a key exchange scheme for secure scheduling of big data applications in. [5] [6] the authors proposed security models to solve authentication, privacy issues in related areas. However, the existing protocols in the related area cannot be directly

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

applied in big data collection [11] in large scale IoV. As a result, the security and efficiency issue for big data collection still deserves.

To overcome above limitations here we used novel frameworks for secure data collection in Vehicular Ad hoc Networks. In this paper, a secure information collection scheme for big data in large scale IoV is proposed. Single sign-on algorithm for authentication are utilized with improved efficiency. The proposed secure data exchange algorithm using message digest and random key contributes to overhead reduction. The business data is transferred in plain text form while the confidential data is transferred in cipher text form. The collected big data will be processed using hadoop architecture to achieve the unified management.

The evaluation result and discussion show the proposed secure information collection scheme achieves high efficiency and security for big data in large scale IoV. In this paper, we propose two security mechanisms to improve the QoS of safety applications in IoV. Based on robustness of the security algorithm, vehicles incur security processing delays that can cause congestion at the security queue.
To overcome this challenge, the first technique picks random level of security at each transmission. The second proposed technique iteratively selects the best possible security level according to a measure of security queue congestion known as cryptographic loss ratio.

III. PROPOSED MEHODOLOGY

Internet of Things (IoT) as a huge interactive network, Internet of Vehicles (IoV) has become an important issue of mobile Internet. Information such as vehicles' location, speed and driven route are collected to central processing system using particular sensors and devices Huge research value and commercial interest will be promised after computing and analyzing vehicles' [7] information Large scale IoV achieves unified management as an extension for IoT in smart transportation area.

In this proposed framework, we used novel schemes for secure transmission and big data collection in Vehicular Ad hoc Networks. Secure information collection scheme for big data in large scale IoV. Single sign-on algorithm for authentication are utilized with improved efficiency. The proposed secure data exchange algorithm using message digest and random key contributes to overhead reduction. The business data is transferred in plain text form while the confidential data is transferred in cipher text form. [8] The collected big data will be processed using hadoop architecture to achieve the unified management. The evaluation result and discussion show the proposed secure information collection scheme achieves high efficiency and security for big data in large scale IoV. In this paper, we propose two security mechanisms to improve the QoS of safety applications in IoV.

Based on robustness of the security algorithm, vehicles incur security processing delays that can cause congestion at the security queue. To overcome this challenge, the first technique picks random level of security at each transmission. The second proposed technique iteratively selects the best possible security level according to a measure of security queue congestion known as cryptographic loss ratio.

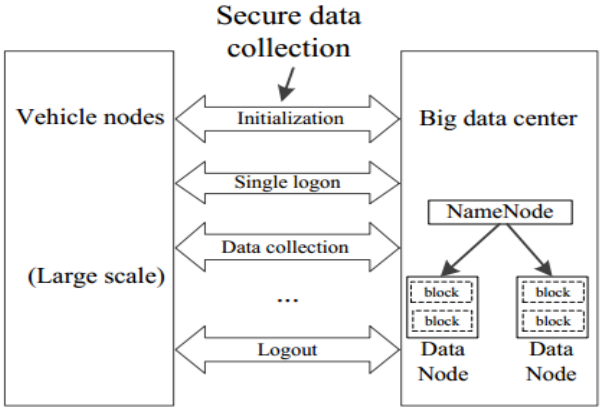

Fig.1 Proposed Scheme

To address the security problems in wide area IoV, a secure information collection scheme for big data is proposed. To begin with, vehicles need to register in the big data center to connect in the network. After the initialization phase, the vehicles associate with the big data center via authentication towards both sides using single sign-on algorithm. The collected information is transferred under security protection with improved efficiency.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

3.1 Proposed Schemes:

3.1.1 IoV

According to particular communication protocols and data interaction standards, IoV is an integrated network based on in-vehicle network, Vehicular Ad Hoc Network and vehicle-mounted mobile Internet. It is an extended application of Internet of Things which achieves intelligent traffic management control, [9] [12] vehicles intellectualization control and intelligent dynamic information service. Vehicle nodes, sink nodes and big data center constitute the basic architecture of the Internet of Vehicle. Vehicle station parameter collection module and so on. As sink nodes, [13] rode side units and users' communication devices help transfer the information. High speed, node topological structure is dynamic and changing. It is hard to build accurate neighborhood.

3.1.2. Big Data

Big Data is a system that let digitize large amount of information and combine it with existing databases. [14][15] Big data is defined based on three primary characteristics, also known as the 3Vs: volume, variety, and velocity. The increasing numbers of vehicles collect data from different places and various attributes, which converge big data of heterogeneous nature with variation in size, volume, and dimensionality. As for the government, the collected big data helps analyses and solve the traffic problems. As for the company like real-time transportation company, it helps optimize the vehicle resource.

3.2.3. Security Requirements for IoV

According to the features of IoV, the secure information collection scheme has to meet the requirements to ensure the data collection security. The security requirements with operational functions and management functions include:
1) Authentication to identify the vehicle node, sink node and big data center; 2) Integrity to protect messages against modification or destruction; 3) Confidentiality to protect the information sent to appropriate entity. The business data like temperature parameters can be transferred in plain text form while the confidential data like location data need to be transferred in cipher text form; 4) Non-repudiation to prevent deny afterward;
To address the security requirements in large scale IoV, a secure data collection scheme for big data is proposed. These data will be collected by big data center with secure protection and stored in distributed storage system using Hadoop architecture [16] [17]. In the initialization phase, association with authentication towards all new adding vehicle nodes forms the first security line of defense against illegal nodes.

3.2 Authentication Phases

3.2.1. Initialization

To support different kinds of big data platform, we assume that each vehicle is equipped with a certificate issued by outside Certification Authority (CA). In the initialization phase, vehicles need to register in the big data center to connect in the network. [18] Vehicle nodes and big data center generate public key and private key of themselves respectively. Certification, with their corresponding public keys as a pat, is exchanged between vehicle nodes and big data center. If the certificates pass the inspection, the corresponding ID will be registered as a valid account. Sink nodes are responsible for message forwarding. What's more, sink nodes are also necessary to register in this phase.

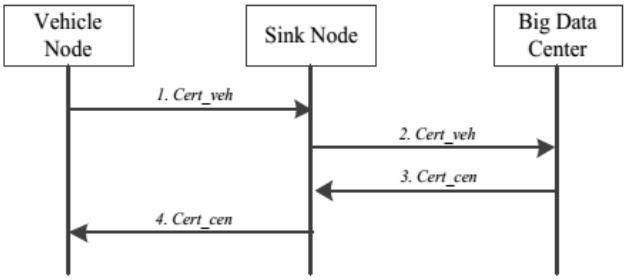

Fig.2 Message Exchange in Initialization Phase

3.2.2 Logon for the First-time

With the development of IoV, an increasing number of vehicles are connected to the network. Vehicles may run at a high speed and connect to different sink nodes. The secure information collection scheme proposed single sign-on algorithm which improves the efficiency of the logon protocol [19]. The expandability is enhanced utilizing the proposed scheme. After initialization phase, sink nodes and vehicle nodes connect to the big data center using different protocol.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

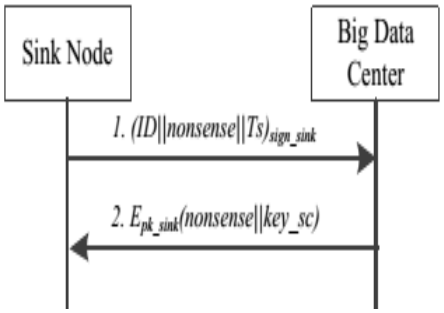

Fig. 3 Sink Node logon for the First time

In the phase of sink nodes' sign-on, ID, nonsense and Ts are sent to big data center with sink nodes' signature as shown in Fig.3. [20] According to received message, big data center checks the signature and ID of sink nodes. What's more, Ts guarantees the time-efficiency while nonsense resists replay attack. If the messages are legal from valid account, the big data center generates the unique keys.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

In this section, we present the simulation results for evaluating the performance of our proposed mechanism. The simulation result of single sign-on algorithm, message digest and random key shows the efficiency in logon process and data collection phase.

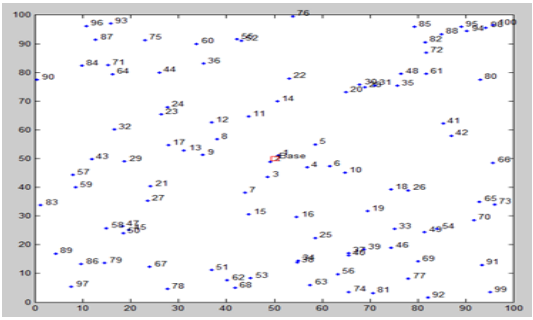

Fig.4.1. Initial Node Assignment (100 Random nodes)

Fig. 4.1 shows the initial node assignment for the nodes placed randomly. Here we have placed 100 nodes in a random way.

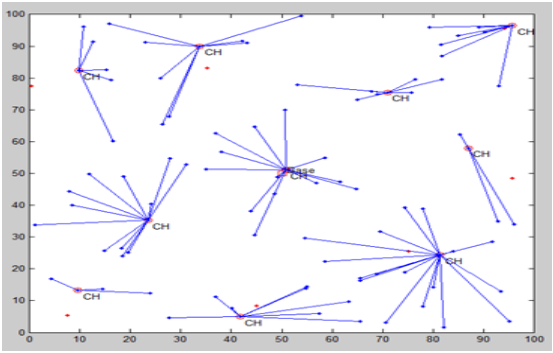

Fig.4.2. Active Detection Routing Protocol

Fig.4.2. shows the active detection of nodes present in a routing protocol. The Active trust algorithm is being proposed here for the formation of nodes.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

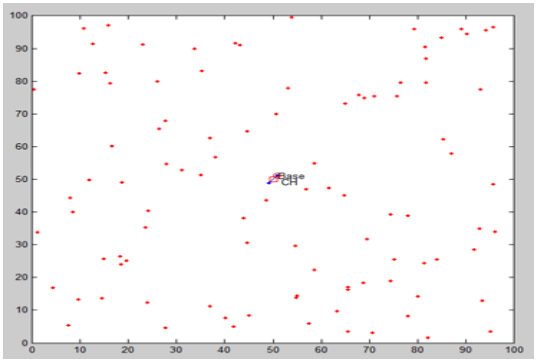

Fig.4.3. After Data Routing Protocol

Fig. 4.3.shows the placement of nodes proposed after the data routing protocol. The nodes of nearly 100 in number are placed randomly.

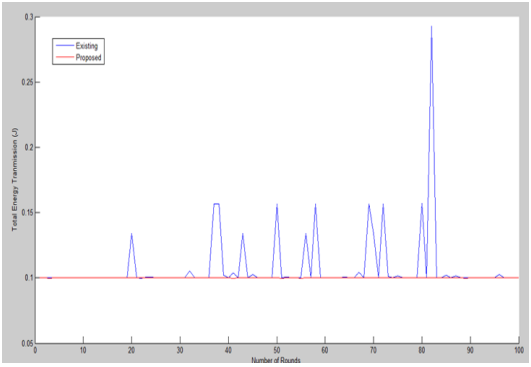

Fig.4.4. Total Energy Transmission vs number of Rounds

Fig. 4.4.shows the comparison of total energy transmission of the proposed and the base work. The existing methodology has large amount of variations where as the proposed has no such variations.

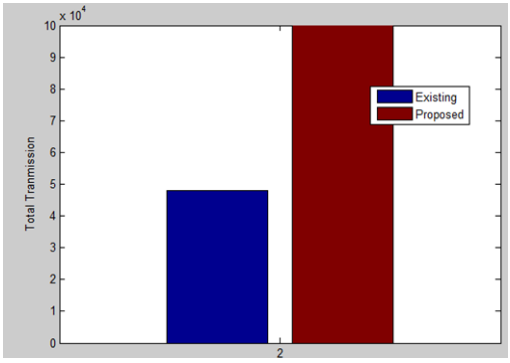

Fig.4.5.Total Transmission Data Volume

Fig.4.5 shows the Total transmission Data Volume for the proposed and existing methodology.

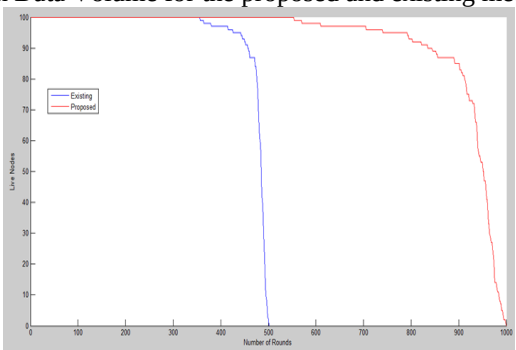

Fig.4.6. Number of Rounds vs live nodes

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

The Fig.4.6 shows the graph which is plotted for number of rounds against the live nodes. The existing methodology could only get 500 rounds in total where as the proposed method can reach upto 1000 rounds.

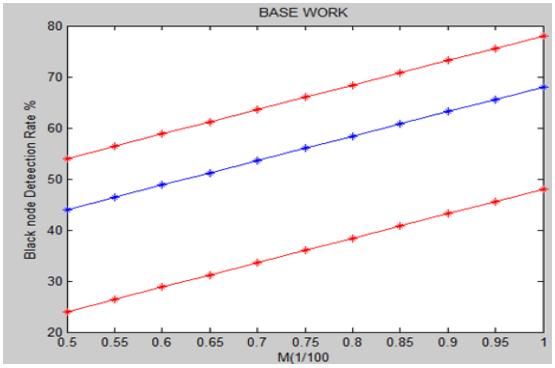

Fig.4.7. BASE WORK Black node Detection Ratio vs Data volume M

Fig. 4.7.shows the Black node detection rate of the base works. The graph is plotted for the Black node Detection Ratio against the Data volume. The maximum data volume produced would be nearer to 80.

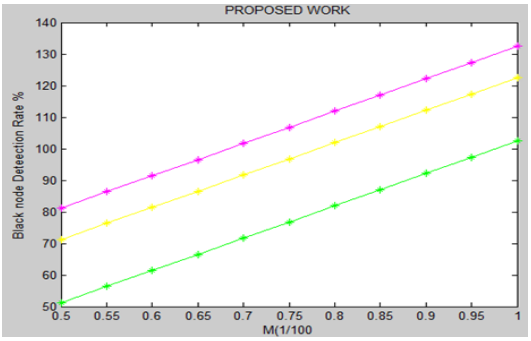

Fig.4.8. Proposed work Black node Detection Ratio vs Data volume M

Fig. 4.8.shows the Black node detection rate of the existing work. The graph is plotted for the Black node Detection Ratio against the Data volume. The maximum data volume produced would be more than 130.

V. CONCLUSION

A secure information collection scheme for big data in large scale IoV is proposed. Single sign-on algorithm for authentication are utilized with improved efficiency. The proposed secure data exchange algorithm using message digest and random key contributes to overhead reduction. The business data is transferred in plain text form while the confidential data is transferred in cipher text form. The collected big data will be processed using hadoop architecture to achieve the unified management. The evaluation result and discussion show the proposed secure information collection scheme achieves high efficiency and security for big data in large scale IoV. In this paper, we propose two security mechanisms to improve the QoS of safety applications in IoV. To overcome this challenge, the first technique picks random level of security at each transmission. The second proposed technique iteratively selects the best possible security. Simulation results show that the proposed techniques significantly improves the application QoS in terms of delay and packet delivery ratio.

In the future, our work will consider developments in the following three aspects. A demonstration experiment is necessary to verify our proposed scheme's efficiency and security. With the increasing amount of vehicles in the IoV, we could do some further research about the routing protocol of IoV to optimize our security scheme. And with the development of the new communication technology, such as 5G, we would pay attention on the security scheme to fit with these changes.

REFERENCES

[1] J. A. Guerrero-ibanez, S. Zeadally, J. C. Castillo, "Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies", IEEE Wireless Communications, vol. 22, no. 6, pp. 122-128, Dec. 2015.
[2] M. Jin, X. Zhou, E. Luo, and X. Qing, "Industrial-QoS-Oriented Remote Wireless Communication Protocol for the Internet of Construction Vehicles", IEEE Transactions on Industrial Electronics, vol. 62, no. 11, Nov. 2015.
[3] N. Kumar, J. J. P. C. Rodriguesand and N. Chilamkurti, "Bayesian Coalition Game as-a-Service for Content Distribution in Internet of Vehicles", IEEE Internet of Things Journal, vol. 1, no. 6, pp. 554-555, Dec.2014.

[4] J. Fu, Z. Chen, R. Sun and B. Yang, "Reservation Based Optimal Parking Lot Recommendation Model in Internet of Vehicle Environment", China Communications, pp 38-48, vol.11, no.6, Oct. 2014.
[5] J. Cheng, J. Cheng, Me. Zhou, F. Liu, S. Gao and C. Liu, "Routing in Internet of Vehicles A Review", IEEE Transactions on Intelligent Transportation Systems, vol.16, No. 5, pp 2339-2351, Oct. 2015.
[6] A. Dua, N. Kumar, and S. Bawa, "A systematic review on routing protocols for Vehicular Ad Hoc Networks," Vehicular Communications, 1, vol. 2014.
[7] B. Li, C. Zhao, H. Zhang, X. Sun, "Characterization on Clustered Propagations of UWB Sensors in Vehicle Cabin: Measurement, Modeling and Evaluation," IEEE Sensors Journal, vol.13, no.4, pp. 1288-1300, Apr. 2013.
[8] N. Kumar, S. Misra, J. Rodrigues, M. S. Obaidat. "Coalition Games for Spatio-Temporal Big Data in Internet of Vehicles Environment: A Comparative Analysis", IEEE Internet of Things Journal, vol.2 no.4, Aug. 2015.
[9] Y. Zhou, S. Chen, Y. Zhou, M. Chen. "Privacy-Preserving Multi-Point Traffic Volume Measurement Through Vehicle-to-Infrastructure Communications", IEEE Transactions on Vehicular Technology, vol. 64, no.12,Dec. 2015.
[10] Q. Wu, J. D. Ferrer, Ú. G. Nicolas. "Balanced Trustworthiness, Safety, and Privacy in Vehicle-to-Vehicle Communications", IEEE Transactions on Vehicular Technology, vol. 59, no. 2, Feb. 2010.
[11] J. Soares, N. Borges, B. Canizes, Z. Vale. "Probabilistic estimation of the state of Electric Vehicles for smart grid applications in big data context", 2015 IEEE Power & Energy Society General Meeting, Denver, July 2015.
[12] K. Mershad, H. Artail, "A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks", IEEE Transactions on Vehicular Technology, vol. 62, no. 2, pp.536 – 551, 2013.
[13] H Wang, B Qin, Q. Wu, L. Xu, J. D. Ferrer, "TPP: Traceable Privacy-Preserving Communication and Precise Reward for Vehicle-to-Grid Networks in Smart Grids", IEEE Transactions on Information Forensics and Security, vol. 10, no. 11, pp. 2340-2351, Nov. 2015.
[14] A. A. Cárdenas, P. K. Manadhata and S. P. Rajan, "Big Data Analytics for Security", IEEE Security & Privacy, Vol.11, no. 6, Dec. 2013.
[15] L.Xu, C. Jiang, J. Wang, J. Yuan, And Y. Ren, "Information Security in Big Data Privacy and Data Mining", IEEE Access, vol.2, Oct. 2014.
[16] M. Rezaei Jam, L. M. Khanli, M. K. Akbari and M. S. Javan, "A Survey on Security of Hadoop", in Proc. 4th International Conference on Computer and Knowledge Engineering (ICCKE), Mashhad , Oct. 2014, pp 716-721.
[17] P. Adluru, S. S. Datla and X. Zhang, "Hadoop Eco System for Big Data Security and Privacy", in Proc. 2015 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY May. 2015.
[18] C. Liu, X. Zhang, C. Liu, Y. Yang, R. Ranjan, D. Georgakopoulos and J. Chen, "An Iterative Hierarchical Key Exchange Scheme for Secure Scheduling of Big Data Applications in Cloud Computing", in Proc. 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. Jul. 2013, pp10-16.
[19] H. Li, Y. Yang, T. H. Luan, X. Liang, L. Zhou, and X. (Sherman) Shen, "Enabling Fine-grained Multi-keyword Search Supporting Classified Sub-dictionaries over Encrypted Cloud Data," IEEE Transactions on Dependable and Secure Computing, 2015.
[20] H. Li, X. Lin, H. Yang, X. Liang, R. Lu, and X. (Sherman) Shen, "EPPDR: An Efficient Privacy-Preserving Demand Response Scheme with Adaptive Key Evolution in Smart Grid," IEEE Transactions on Parallel and Distributed Systems, 2014, vol. 25, no.8, pp. 2053 - 2064.