Volume 5, Issue 8, August 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Study on Cooperative Node Selection Issues in Sensor Network Routing

Garima*
M.Tech, ECE Deptt., NCCE
Panipat, Haryana, India

Deepti Jaglan
Senior Lecturer, ECE Deptt., NCCE,
Panipat, Haryana, India

Abstract - Sensor network is the real time network defined under application specific and environment specific constraints. The restricted node level and network level constraints increase its complexities. The network is composed under architectural specifications. While forming the communication and gaining the optimization, it is required to consider the associated issues. These issues provide the setting up constraints and communication decision at earlier stage so that the preventive network level and environment level adjustments can be done. In this paper, some of the sensor network issues are presented and discussed. The paper also discussed some of the methods for link quality estimations so that the cooperative node selection will be done.

Keywords - WSN, Criticalities, Issues, Architecture , Communication.

I. INTRODUCTION

A sensor network is scenario specific real time network .The nodes in the network are static and defined in the restricted and defined network scenario. The restrictions are here applied in terms of energy restriction and architectural specifications. The capabilities of the nodes are required to explore so that the optimized communication will be performed. To understand this, it is required to identify the basic features of the network under which the architectural formation is done. Here figure 1 is showing the associated features to the network.

The first and foremost constraint defined for the sensor network specification is the architectural constraint. The network is composed under the specific architectural definition. This architectural includes the network level, node level and environment level parameters. One of such common network architectural is clustered architecture. In this architectural form, the network is divided in smaller sections called clusters. Each cluster is defined with relative cluster controller. The controller manages the communication within cluster as well as manages the communication between the clusters. Architecture is the aggregative communication architecture in which network nodes are connected under some aggregative operator to provide the communication in the network.

Another network feature is cooperative communication in network. The cooperative communication gives the dynamic and infrastructure less communication. In this communication form, each node identifies the neighbor nodes in the defined sensing range. The decision under different parameters is taken to identify the next cooperative neighbor node. This analysis includes the selection of next communicating host in the network. Another feature and the criticality to the network is the restricted resource network. The sensor nodes are defined under the energy specification. The initial energy of the network nodes is defined as well as the as the energy consumption vector with each communication is defined. The communication between two nodes depends on the energy of source and destination node. This communication also dependent on the distance between the node pair and the type of information over the network. These all vectors collectively affect the network life. The network nodes are the energy nodes and the collective energy of nodes defines the network life. The communication performed in the network gives the energy loss and degrades the network life. As the network is optimized, it basically improves the network life.

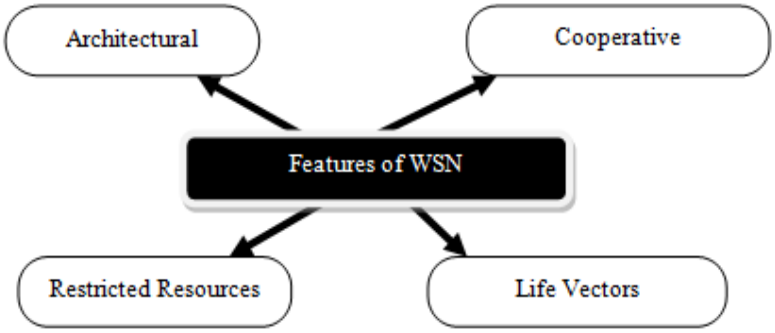

Figure 1 : Reasons of Security Threats in WSN

In this paper, a study to the network challenges and features is defined. The network has provided the cooperative communication constraints so that the adaptive and the reliable communication will be formed. In this section, the sensor network is described along with network features. In section II, the work defined by the earlier researchers is discussed. In section III, the cooperative communication issues and constraints are discussed. In section IV, the conclusion obtained from the work is presented.

II. LITERATURE REVIEW

A sensor network is the critical network defined under the energy constraints and the restricted network specifications. The network suffers from different network threats including the energy level and security level features. In this section, some of the contributions of earlier researcher are discussed. Axel Krings has provided [1] a work on neighborhood monitoring to provide the cooperative communication and for effective neighbor selection mechanism. Author provided the constraint and the limitation driven network so that the optimized neighbor selection will be done. Author provided the work on malicious node selection under dynamic constraints so that the optimized communication will be formed in the network. Ying Li provided [2] a work on the malicious node identification model in cooperative communication network. The network is defined under the mathematical modeling applied in the scenario specific network. The network is defined under the probabilistic measure and framework so that the attack restricted network formulation will be done. Bogdan Carbunar provided [3] a secure routing model under neighbor reliability identification. Author provided the communication constraint analysis to separate the reliable and the attacked nodes in the network. The infrastructure specification and relative identification of neighbor nodes with malicious node constraints is defined in the network. The route formation under restricted network constraints is defined in this work.

Johann Schlamp [4] provided a work on route formulation method under hijacking attack model. Author provided the neighbor node analysis with specification of cooperative node nature and identify the spam nodes to form the reliable communication. Author provided the packet formation and packet prefix analysis to provide the reliable packet communication. Author provided the incidental communication analysis from the cooperative communication analysis so that the victim induced communication will be performed over the network. Joshua Goodman [5] defined a work on the secure and reliable communication under control communication method. Author provided the conventional communication while restricting the spam packets and providing the safe and secure communication. The cooperative node analysis is provided by the author under the neighbor strength formulation with profit derivation and the reliability estimation. The reliability is here obtained under the energy and the security constraint specification. These all parameters are collected under profit driven model to achieve maximum communication gain. Danny Dhillon [6] has provided a work on integrity level analysis to identify the attacked node in the network. The safe node level analysis on the neighboring node analysis is applied with communication schedule formulation and the decision rate identification. The node level effectiveness are rated and a complete communication schedule in prioritized manner is generated. This schedule formulation is done to identify the next reliable and effective neighbor. As the node is selected, the communication is performed over that reliable node. Ahmed Khurshid [7] has provided a work on the real time network scenario to provide the selection of the neighbor node selection under the communication to identify next forwarding node. The reliability is here based on multiple intact parameters and the selection is done under throughput level and rate level selection. This node selection is done for communication level optimization. Evan Cooke [8] has provide the traffic level analysis applied on the nodes defined in the communication range. The packet loss is analyzed under the infrastructure specification for forming the opportunistic network. This network formulation is done to generate the neighboring node so that more reliable and effective communication will be formed. Author[9] provided network level formulation is provided to achieve the linear communication mechanism. Author analyzed the neighbor nodes under communication constraint with optimal communication and constraints formulation. The communication flow analysis is provided to achieve the maximize communication in optimal network conditions. Author provided the communication flow analysis to achieve the safe and reliable communication route. Mauro Conti [10] provided a work on the replication network formulation and to provide the attack preventive route generation over the network. Author provided the constraint specific analysis on the neighboring nodes so that the reliable communication will be obtained from the network.

Garima Gupta [11] has provided a communication scheme under attack specific characterization. Author provided the delay and the attack preventive communication method to form the network route. Author provided the algorithmic formulation for route generation. Author presented a probabilistic measure for behavior analysis applied on the neighboring nodes for effective and reliable cooperative node selection. The communication solution is provided under the neighbor aware communication method. Author[12] provided a security aware communication model to achieve the communication optimization in restricted network. Author provided the attack level analysis in a false detection rate and achieves the network reliability with impact specific analysis. Author provided the overhead analysis for communication level optimization. Peter J. J. McNerney [13] provided the dimensional analysis applied in the network for route formulation and the neighbor node adjustment and route level optimization. Author provided the QoS optimization under the path formulation and multipath adaption in the network. Author provided the bandwidth driven analysis to achieve the communication level optimization in the network.

III. CHALLENGES IN COOPERATIVE NODE SELECTION

The sensor network is the infrastructure less network in which the communication is performed through the cooperative nodes. In different network architectures, the communication is performed over the multi hop path. The election of the

next neighbor to perform the communication is always a challenge. This challenge depends on the associated node level, network level parameters. The issues and the restriction relative to the network nodes for cooperative node election are shown in figure 2.

A) Node Localization

A sensor network is the real time network defined under the application and environmental condition. The node and the network position and localization affects the communication performed in the network. A node localized in the critical network region cannot be selected as the intermediate communication node. The localization of the node actually represents the architectural specification of the node including the actual node position, required bandwidth, communication range, communication requirement, communication restrictions etc. Based on the localization the node constraints are defined at the time of network setup. The node localization can be static or dynamic.

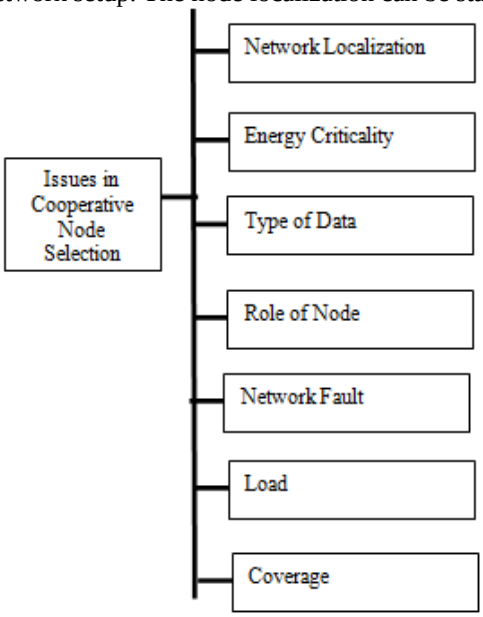

Figure 2 : Challenges in Cooperative Node Selection

In case of intelligent localization, the positional change is performed based on the communication strength and localization parameter analysis. The architecture level improvement can be achieved by applying the dynamic location.

B) Energy Criticality

The sensor network is actually the energy specific network model in which the nodes are defined with energy specification and restriction. The network life is also defined in terms of aggregative energy in the network. As the communication performed some amount of energy is lost on each node. The energy specification on nodes represents the life and considered as the parameter to analyze the network effectiveness and reliability.

C) Type of Data

In a sensor network, different nodes can perform different type of communication. This communication type variation can be defined in terms of type of communicating data. The data can be discrete or the continuous. The continuous data communication can be applied to provide the data modeling and to provide the safe communication in the network. The network modeling is here provided under the video type communication. Higher the criticality of data, more effective architectural and the routing specification is required.

D) Role of Node

The role of a node is defined as the constraint respective to which the communication in the network is formed. The node level and the network level capabilities are defined by the node. As the sensor network is implemented in the real time critical network so that that the role is also based on the application constraints. Generally this role is pre-defined and applied in the heterogeneous network. This role defined the node localization, type of information collected and communicated in the network. The role also represents the criticality of the network.

E) Network Fault

As of any network, the sensor network also suffers from the attack level or the fault level criticalities. If no attack occur in the network, but the network always suffers from the changes of fault occurrence because of the energy level restriction over the network. As the communication initiate in the network, it is required to perform under the node level and the communication level constraints. The communication distance, node criticality, region criticality, energy collectively can form the network fault. To achieve the reliable communication in the network, fault preventive communication is required. Higher the probability of communication fault , lesser the reliability of the network itself.

F) Load

As the nodes are defined with different roles under the application and the architecture specification, based on this role, the load of the network can be identified. The number of parallel communications performed on a node can be identified as the node load. The load on a node increases the node criticality. It not only increases the energy consumption on that particular node but also increases the communication criticality. The number of communication instances over a node increases the criticality of node and increases the chances of communication fault. While identifying the cooperative node, it is required to discuss the load parameter so that the effective neighbor selection will be done.

G) Coverage

The node level coverage is provided to achieve the effective and reliable communication in the network. The coverage is provided to identify the node strength and the communication alternatives so that the safe and the reliable communication will be formed in the network. The communication load also dependent on the coverage parameters. The cooperative node selection depends on the coverage parameters. A node not defined in the coverage of other node is identified as the orphan node and degrades the communication reliability. The optimized coverage improves the strength of cooperative communication in the network.

IV. LINK QUALITY ESTIMATION

The cooperative communication is about to identify the effective next hop. This hop selection is based on certain methods and properties. In this section some of the common methods adopted by different researchers for link quality are described.

A) Passive Link Estimation

This kind of link estimation includes the analysis in terms of overhead identification under static parameter. The periodic update messages are not required for link estimation. This kind of link estimation covers two major phenomenon. The first, it reduces the energy consumption in link estimation and dynamic observation so that more effective link will be identified. The link quality estimation is here applied under data transfer so that the interval specific estimation is required. The stability analysis based link estimation is performed. The throughput analysis at protocol level is performed based on the data rate and bandwidth parameters. This kind of link estimation includes node level parametric observations so that more effective and adaptive link formulation will be done.

B) Packet Reception Rate

This kind of link estimation is based on the receiver side based on throughput level observation. The busty communication analysis is provided at the direction communication rate and relationship observations so that the high reception rate will be achieved. This kind of observation includes the throughput analysis and the communication link observation along with link support estimation and maximum throughput analysis. The receiver side estimation reduces the failure probability so that more reliable link observation can be done. This observation us dependent on communication rate and the link support analysis dynamic. This dynamic nature is identified periodically and presented as the metric based on which the link formulation under strength criteria can be done.

C) Agile Link Assessment

This kind of link assessment is under instability and communication variance analysis. This kind of link estimation is based on static and dynamic parameters. This assessment is under radio link quality as well as short term periodic analysis. The physical and communication parameters are observed collectively to form the link under parametric observations. The link strength and quality indicators are defined to estimate the link and to provide effective reception rate. The signal power level estimation and correlated reception rate along with receiver sensitivity is analyzed for effective hop election. This process is defined along with receiver specific observation applied under node analysis applied under physical and communication strength. The energy level estimation and the noise ratio are also observed for representing the strength and limits of a node. This high correlation estimation and link reliability observation under poor quality is adopted so that the effective relationship will be formed. The observation is performed on sender and receiver side so that more effective relational observation will be summarized. This conditional estimation is applied to derive the effective node so that the effective links will be formed.

IV. CONCLUSION

In this paper, the challenges and the characteristics of the cooperative communication in sensor network are discussed. The study paper is defined to identify the communication and architectural constraint specific discussion so that the communication formulation will be done effectively. The paper discussed the associated features and challenges. The paper also defined some of the methods for link quality estimation. These methods are based on the static and dynamic observations. The route formulation and other network optimization can be derived under these methods.

REFERENCES

[1] Axel Krings," Neighborhood Monitoring in Ad Hoc Networks", CSIIRW ’10, April 21-23, 2010, Oak Ridge, Tennessee, USA ACM 978-1-4503-0017-9.

[2] Ying Li," Component-Based Track Inspection Using Machine-Vision Technology", ICMR’11, April 17-20, 2011, Trento, Italy ACM 978-1-4503-0336-1/11/04.

[3] Bogdan Carbunar," JANUS: Towards Robust and Malicious Resilient Routing in Hybrid Wireless Networks", WiSe'04, October 1, 2004, Philadelphia, Pennsylvania, USA. ACM 1-58113-925-X/04/0010.

[4] Johann Schlamp," How to Prevent AS Hijacking Attacks", CoNEXT Student'12, December 10, 2012, Nice, France. ACM 978-1-4503-1779-5/12/12.

[5] Joshua Goodman," Stopping Outgoing Spam", EC'04, May 17–20, 2004, New York, New York, USA. ACM 1-58113-711-0/04/0005.

[6] Danny Dhillon," Implementation & Evaluation of an IDS to Safeguard OLSR Integrity in WSNs", IWCMC'06, July 3–6, 2006, Vancouver, British Columbia, Canada. ACM 1-59593-306-9/06/0007.

[7] Ahmed Khurshid," VeriFlow: Verifying Network-Wide Invariants in Real Time", HotSDN'12, August 13, 2012, Helsinki, Finland. ACM 978-1-4503-1477-0/12/08.

[8] Evan Cooke," Toward Understanding Distributed Blackhole Placement", WORM'04, October 29, 2004, Washington, DC, USA. ACM 1-58113-970-5/04/0010

[9] Umair Sadiq," CRISP: Collusion–Resistant Incentive–Compatible Routing and Forwarding in Opportunistic Networks", MSWiM'12, October 21–25, 2012, Paphos, Cyprus. ACM 978-1-4503-1628-6/12/10.

[10] Mauro Conti," A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Speed networks", MobiHoc'07, September 9-14, 2007, Montréal, Québec, Canada. ACM 978-1-59593-684-4/07/0009.

[11] Garima Gupta," Reference based approach to Mitigate Blackhole Attacks in Delay Tolerant Networks", Q2SWinet'12, October 24–25, 2012, Paphos, Cyprus. ACM 978-1-4503-1619-4/12/10.

[12] Abhijit Das," Energy Aware Topology Security Scheme for Sensor Adhoc Ad Hoc Network", ICCCS'11, February 12–14, 2011, Rourkela, Odisha, India. ACM 978-1-4503-0464-1/11/02.

[13] Peter J. J. McNerney," A 2-Dimensional Approach to QoS Provisioning in Adversarial Sensor Adhoc Ad Hoc Network Environments", MSWiM'12, October 21–25, 2012, Paphos, Cyprus. ACM 978-1-4503-1628-6/12/10.

