Improving the Quality of Service and Privacy by Integrating Dijkstra's, SafeQ and Extended Watchdog Algorithm in Wireless Sensor Networks

Rakesh K.K, K.Pradeepa

ABSTRACT--- The fundamental issue is framing the sensor nodes and steering the information from sender node to receiver node in wireless sensor networks (WSN). To resolve this major difficulty, clustering algorithm is one of the accessible methods employed in wireless sensor networks. Still, clustering concept also faces some hurdles while transmitting the data from source to destination node. The sensor node is used to sense the data and the source node helps to convey the information and the intended recipient receives the sensed information. The clustering proposal will choose the cluster head depending on the residual energy and the sensor utility to its cluster members. The cluster heads will have equal cluster number of nodes. The complexity is generated in computing the shortest path and this can be optimized by Dijkstra's algorithm. The optimization is executed by Dijkstra's shortest path algorithm that eliminates the delay in packet delivery, energy consumption, lifetime of the packet and hop count while handling the difficulties. The shortest path calculation will improve the quality of service (QoS). QoS is the crucial problem due to loss of energy and resource computation as well as the privacy in wireless sensor networks. The security can be improvised in this projected work. The preventive metrics are discussed to upgrade the QoS facility by civilizing the privacy parameter called as Safe and Efficient Query Processing (SAFEQ) and integrating the extended watchdog algorithm in wireless sensor networks.

Keywords: ***Privacy, Integrity, SafeQ, Dijkstra's, SafeQ, Watchdog***

I. INTRODUCTION

Current advancements demonstrate that they can be proficiently utilized for QoS provisioning. The capacity of little, minimal effort gadgets called sensor hubs to agreeably screen physical or ecological conditions, for example, weight, dampness, the temperature has expanded their significance. The work will follow the endeavors to create QoS-empowered models on WSN systems. Thus, serving dependable and opportune data is a key interest to any WSN. WSN has wide scope of uses in military, natural checking, medicinal services, observing and reconnaissance. In spite of the fact that it can possibly turn into the most proficient answer for QoS provisioning in WSNs, current improvement shows that there are as yet numerous issues and provokes that should be survived [4]. In any case, they consider QoS just as layer explicit detached arrangement of issues and they are exceptionally reliant on the exhibition of different layers.

Wireless Sensor Networks (WSN) is a key territory of new speculations and examinations. It serves an enormous number of users that can be exceptionally basic to the degree of sparing human life. Therefore clients and applications are winding up all the requests. Wireless Sensor Networks has been recognized as the most significant innovation for low control remote correspondence. In this work, two principal approaches are reviewed for QoS provisioning in WSNs: layered and cross-layer approach. Since the idea of the QoS is generally new in WSNs, there are not countless licenses at present managing this issue, in any case yet in coming years an enormous increment in the number of such licenses is normal. Quality of Service (QoS) in WSN talks about certain systems and necessities to give such dependable and confided in administration [2]. Fast propels in Wireless Sensor Networks (WSNs) show that they are winding up progressively unpredictable. It guarantees another space in transit PCs and people interface with our condition.

WSN has additionally utilized continuously applications, the transmission of imaging and video information requires cautious taking care of so as to guarantee that start to finish postponement is inside the satisfactory range and that the variety in such deferrals is adequate so dependability and practicality end up significant QoS parameters progressively applications. Vitality protection is a significant issue to be considered. The constrained memory, low power and restricted handling nature of WSN force a few issues moreover. QoS provisioning with layered methodology is reviewed in three WSN layers: MAC, system and transport layer [3]. Visual Sensor Networks that includes cameras are likewise developing the type of WSN for ongoing applications.

QoS has turned out to be a significant theme in WSN. Because of the remarkable attributes of WSNs, similar to little measurements and constrained assets and capacities, Quality of Service (QoS) is forced as one of the key elements of WSNs. Cross-layer approach does not have the limitations as layered methodology and consequently can arrange with data from all layers of the correspondence convention stack. Initial, a prologue to QoS in conventional systems expressing its parameters and procedures is displayed trailed by basic audit of WSN and its interesting attributes [1].

Revised Manuscript Received on October 15, 2019

Rakesh K.K, Ph. D Research Scholar, Department of Computer Science, AJK College of arts and Science, Affiliated to Bharatiyar University, Coimbatore, Tamilnadu, India.

Dr.K.Pradeepa MCA.,M.Phil.,M.E.,Ph.D, Dean - Department of Computer Science, AJK College of Arts and Science, Affiliated to Bharatiyar University, Coimbatore, Tamilnadu, India

Energy Aware QoS routing protocol (EAQoS) is QoS convention for continuous traffic. The traffic way dependent on cost capacity is found in various ways. It likewise boosts throughput for non-ongoing traffic. Lining model is utilized which partitions the traffic into Real Time and Non-Real Time and assigns data transfer capacity as indicated by estimation of r (Bandwidth proportion). The ideal way is found thinking about vitality for constant utilization and mistake rate while considering start to finish defer required for continuous information. Ways are found and Dijkstra's calculation ways are masterminded by their least cost.

II. RELATED WORK

Stretching out QoS to remote systems introduces new difficulties because of radio channel qualities, portability the board [12], higher misfortune, battery influence compels and low transfer speed [13]. Be that as it may, most current QoS conventions can be actualized in remote neighborhood (WLAN) with some change in light of the fact that the last jump is the main remote stage in these systems. In remote systems like Ad hoc remote systems or the new rising remote sensor systems which are absolutely remote, another arrangement of QoS parameters, instruments and conventions are required.

In conventional systems, similar to the Internet, the QoS can obtained through the system over-provisioning, traffic building, and differential bundle treatment inside switches, as portrayed in [14]. Customarily, the accentuation is on augmenting start to finish throughput and limiting deferral. Over-provisioning of system assets depends on including gigantic measures of assets in the system. Be that as it may, data transmission accessibility and switch limit are not vast assets and abundance assets are costly, particularly in remote systems.

III. MATERIALS AND METHODS

3.1 Dijkstra's Algorithm

The relative location of all the sensors can be evaluated by applying a shortest path method called as Dijkstra's algorithm with low cost. The prevention of errors is effective in this method [6]. The theory is stored in the routing table and the performance of location evaluation and measuring the distance among the sensor fields. The algorithm helps to analyze the finest paths i.e. shortest course of travel from source to destination.

Here the source and destination nodes are denoted as S and D. The routing algorithm builds a routing table to store the weights of each node to find the shortest path. The fields like antecedent field, field length and field label. When there is no direct connection among the source and destination, then it is represented as infinity [5]. The steps are listed below and given in figure 1:

Step 1:

The fields are:

- Antecedent field – to list the previous node
- Field Length – the sum of the weights are Calculated from source to next node
- Field Label – eternal or uncertain

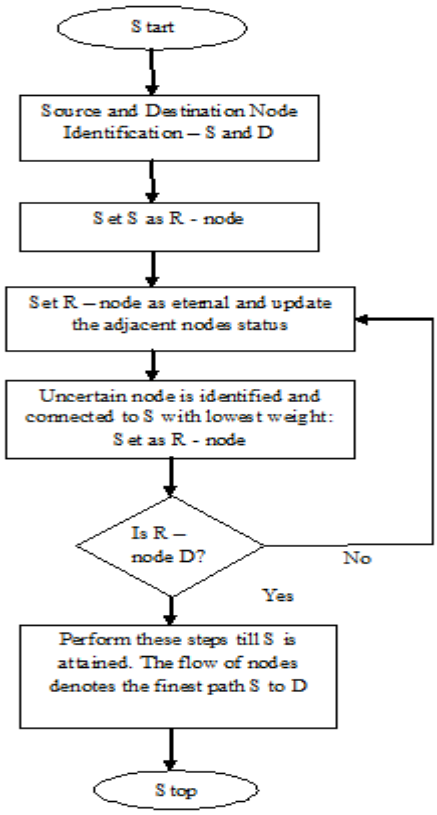

Figure No: 1 Dijkstra's Algorithm

Step 2:

Then the parameters are initialized and the labels are set be either uncertain and the length is said to be infinity.

Step 3:

In this period, the router is set to be R –node. If S is the source R – node the label can be changed. The labels are changed from uncertain to eternal. The changes cannot be modified after execution.

Step 4:

The routing updation are performed and they are connected directly to source R – node.

Step 5:

Next stage is to choose the node which has the lowest weight. The router will travel over the uncertain nodes and then the lowest weight of the node is chosen. This might be the destination D node.

Step 6:

If suppose, the chosen node is not D (exact destination node) then again go back to step 5.

Step 7:

Suppose the identified node is destination node, then the previous node can be extracted from record and this process gets executed till it attains S node. This helps to show the finest route i.e. shortest route from S to D. The relative advantage is to determine the shortest path and it gives great accuracy.

3.2 SafeQ

The sensor network architecture is illustrated in figure 2. It is comprised of sink, sensor nodes and storage nodes. Sensors are not expensive but it has more computing power with restricted storage [8]. Storage nodes are more powerful and the power of computing more than sensor nodes. The closest storage is selected to send the data from the sensor node. The sink is the node for user contact of the sensor node. The user will acquire the query and in turn it they get converted into numerous queries and they get separated to the storage nodes and then the results are given back to sink node. The sink node will clarify the result and the final results are provided to the user.

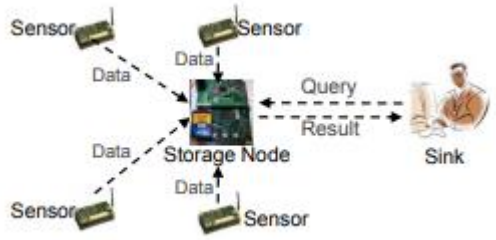

Figure No: 2 Sensor Network Architecture

The sensor architecture is not a trusted model. Hence there is a necessity of privacy and security among the nodes in the network. The storage node acts as a mediator between sink and sensor nodes. The queries are processed and stored here. The efficacy of the storage is more powerful for query processing. But there is no privacy and trust among the nodes in the network.

The storage nodes are more complex for the users because it is more reliable to intruders. Hence the called as "Secure and Efficient Query Processing in Sensor Networks (SafeQ)" is designed for providing security and integrity. The method helps to offer integrity, authentication and quality of service. The privacy can be preserved to detect the intruders from processed queries [7]. The sink node helps to identify the protective storage nodes. The privacy is handled by encoding the queries and the information can be encoded by utilizing the table values given in routing table. Also the integrity can be maintained by the adjacent nodes that permits sink to verify the query results and the data items.

The method is,

- The method employs digital signature concept for affording authentication
- Any type of asymmetric encryption can be performed for confidentiality
- Privacy and integrity is preserved by SafeQ method for handling the queries efficiently
- Then the watchdog mechanism is used to detect the behaviour of malicious nodes.

3.3 Watchdog

Watchdog algorithm is employed to detect the mischievous nodes in the network for delivering the packets more securely among various nodes. Each network will include the watchdog algorithm to analyze the nature of its adjacent nodes and the watchdog node will acquire the information about packet transmission. In the given figure 3, the natures of various nodes are examined [10]. Here 'S' is denoted as watchdog to gather the information about adjacent nodes A, B, C and D. The node 'S' will send the packet to its neighboring node 'A' and 'S' acts as watchdog. Then the node 'A' will broadcast the data to 'B' and the 'S' will make sure that the data has been reached from 'A'. But the method suffers from various disadvantages which fail in discovering attacker nodes.

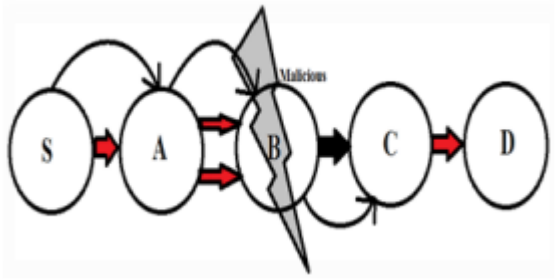

Figure No: 3 Theory of Watchdog

The disadvantages are: a) collision – When A coveys the data to B and then to C, collision may occur. And when any data enters from S then the node 'A' fails to eavesdrop on 'C'. Hence the mischievous node cannot be identified easily. b) Power Transmission - When the node starts receiving the data, the power transmission may gets dropped in the middle. c) Dropping the packets – When the eavesdropping occurs, the some data cannot be handled properly then the packet dropping may occur [9]. Hence the method can be improvised by including the HALT, ACKNOWLEDGEMENT, NUMBERING and DETECTION graph methods [11].

i) HALT

The mechanism is utilized when there is more traffic. The concept of collision can be eliminated by HALT theory. When the data gets transmitted from source to destination and next information cannot be transmitted. The receiver node must offer the acknowledgement message to sender and it should be in halted mode till it gets the acknowledgement. The halt procedure will not permit other nodes to convey the information. If the acknowledgement is not received, then the node is considered to be malicious. The major drawback of watchdog can be resolved by HALT mechanism. When the information is broadcasted from B to C then the acknowledgement has to pass by C and the process has to be halted and it eavesdrops the transmitted message. The method is delineated in figure 4.

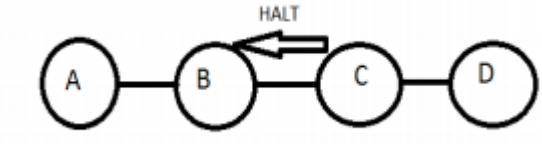

Figure No: 4 HALT Procedure

ii) ACKNOWLEDGEMENT

The process minimizes the problem of power transmission as well as collision. When the message is

passed from the A to C then the acknowledgement must given by C to A until then the process has to be halted before sending the other information. Since the process gets halted, the process of dropping the packets may not happen and eavesdropping can be implemented successfully. Hence the accuracy can be enhanced by resolving the collision and power transmission. The illustration is given in figure 5.

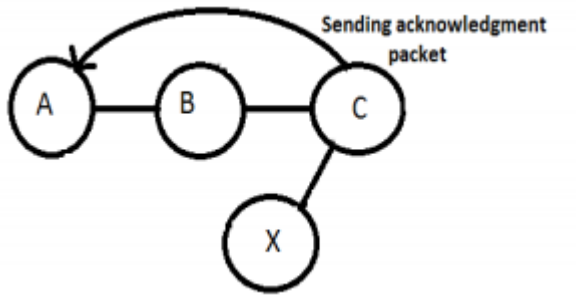

Figure No: 5 ACKNOWLEDGEMENT Procedure

iii) NUMBERING

The efficacy of the algorithm can be enhanced and the mischievous nature can be minimized by numbering method. The counter is introduced to increase the value of the node. When the information is conveyed from one to another node then the source node will get incremented. After transmitting the information and the value is not incremented then the node is said to malicious node.

iv) DETECTION Graph

The problem of packet dropping can be eradicated by watchdog method. The traffic maintenance is handled by detection theory. When the packets are dropped by the mischievous node, the malicious node is detected by the number of inflow and outflow packets from source to destination. The malicious node is found by considering the inflow and outflow traffic rate. When outflow is greater than inflow value then the node is not malicious. In the given figure 6, the outflow keeps on decreasing as it is passed from source to destination and hence the nodes are considered to be mischievous.

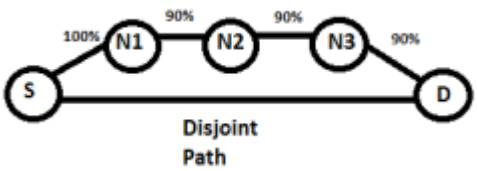

Figure No: 6 DETECTION Procedure

IV. RESULTS AND DISCUSSION

Since the network is comprised of minimal power computing devices and that is scattered among the isolated regions. Sensors will acts as a clusters and the cluster head helps to convey the sensed data to base station. The sensors are entrenched with batteries and hence the consumption of energy occurs, which seems to be the crucial concern in WSN. Therefore the consumption of energy can be minimized and the lifetime of the network can be extended by expanding the clusters for energy balance among the sensor nodes. Along with the clusters, Dijkstra's algorithm is employed to find out the shortest path in wireless sensor networks. Since the shortest route is examined, the obstacles can be avoided. The Dijkstra's method is evolved to minimize the consumption of energy. The energy consumption measures are depicted in table 1 and figure 7.

Table No: 1 Energy Consumption

Packet Size (bytes)	Time (ms)	
	EAQoS	SAFEQ
0	0	0
20	3	7
40	5	9
60	3	7
80	5	10

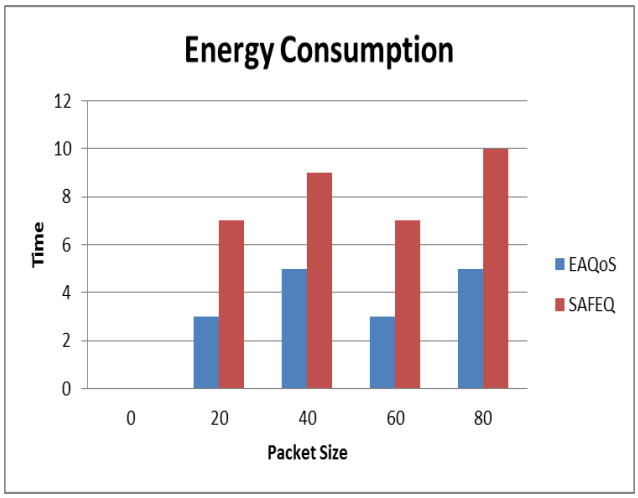

Figure No: 7 Energy Consumption

The projected method is the combination of Secure and Efficient Query Processing in Sensor Networks, Dijkstra's algorithm and Watchdog algorithm. The method consists of privacy as well as shortest path computation. The intruder zones are identified by security algorithms like Secure and Efficient Query Processing in Sensor Networks and Watchdog algorithm which helps to preserve the integrity of data. When Dijkstra's algorithm is integrated with privacy the energy efficiency is enhanced. This also helps to maximize the life span of the network. The energy efficiency is figured out in table 2 and figure 8.

Packet Size (bytes)	Time (ms)	
	EAQoS	SAFEQ
0	100.00	100.00
20	90.672	97.538
40	82.657	92.523
60	70.122	78.682
80	64.282	82.420

Table No: 2 Energy Efficiency

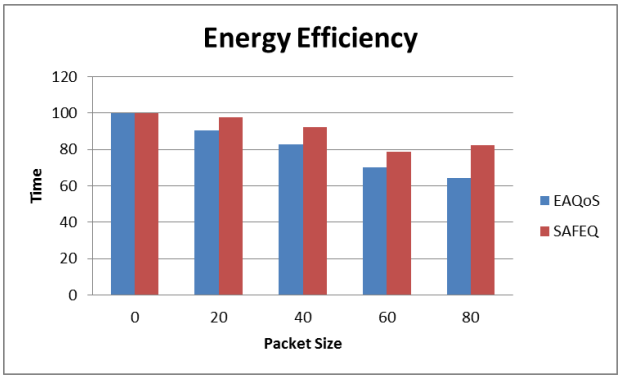

Figure No: 8 Energy Efficiency

Next parameter is Packet Delivery Ratio (PDR). It is the total number of packets shared between source and destination. The authentication is effectively performed by SafeQ and watchdog method. Hence the packet delivery can be improvised. The packets can be forwarded quickly from source to destination by determining the shortest route by Dijkstra's algorithm. The reliability of the network is also enhanced. The output is described in table 3 and figure 9.

Packet Size (bytes)	Time (ms)	
	EAQoS	SAFEQ
0	0	0
20	24.223	30.423
40	48.125	54.562
60	72.632	80.627
80	84.638	98.319

Table No: 3 Packet Delivery Ratio (PDR)

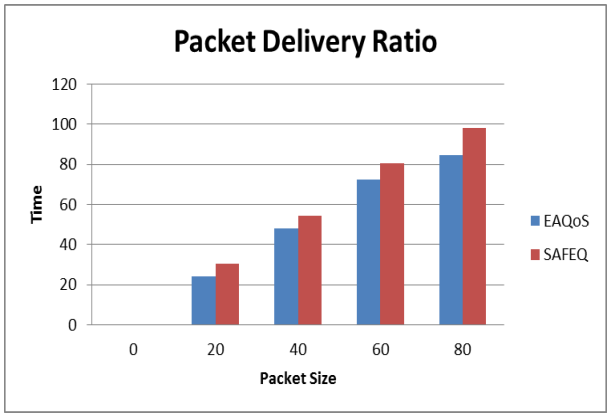

Figure No: 9 Packet Delivery Ratio

Another important criterion is throughput. It denotes the specified number of data units processed in a given period of time. This parameter helps to calculate the amount of information delivered effectively. The cluster head can be rotated to enhance the throughput by considering the levels of threshold among the sensor nodes and that helps for dropped packet reduction. The throughput is given in table 4 and figure 10.

Packet Size (bytes)	Time (ms)	
	EAQoS	SAFEQ
0	0	0
20	56.213	75.321
40	102.123	130.175
60	140.827	188.683
80	164.221	265.301

Table No: 4 Throughput

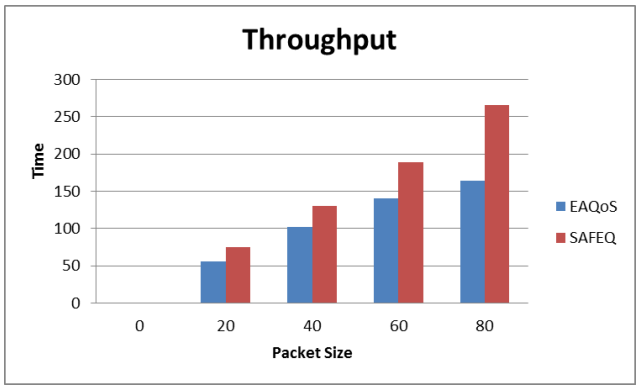

Figure No: 10 Throughput

The overhead is the total packets required for communication in the network. This is computed by taking the total packets sent which is divided by total number of packets received in the destination side.

Packet Size (bytes)	Time (ms)	
	EAQoS	SAFEQ
0	0	0
20	74.221	64.201
40	133.285	110.239
60	189.683	180.212
80	267.301	201.857

Table No: 5 Routing Overhead

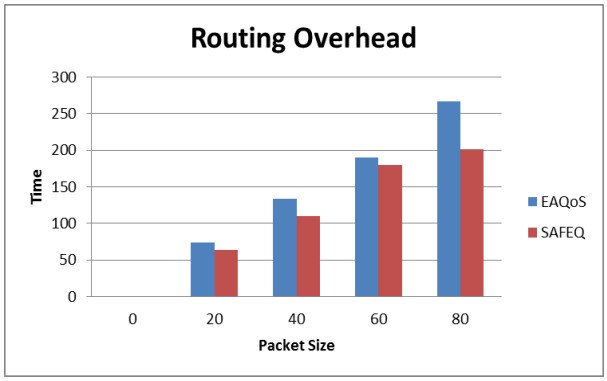

Figure No: 11 Routing Overhead

This parameter can be resolved by utilizing the finding the minimal distance to transmit the packets. Since the shortest path is determined, the routing overhead can be resolved. The routing overhead is illustrated in table 5 and figure 11.

V. CONCLUSION

Thus the quality of service can be upgraded by combining the Dijkstra's algorithm, SafeQ and extended watchdog method. Qos can be computed and enhanced by computing the shortest path by Dijkstra's algorithm. The node which has the minimum weight is taken to find the finest route from source to destination. The finest route identification resolves the problem of Quality of Service. Even though the Qos is solved, it cannot solve the problem of privacy. The privacy, security and integrity constraints can be resolved by SafeQ and extended watchdog algorithm. The security parameter determines the malicious nodes and hence the attacks can be prevented. Thus the projected method will ensure the Quality of Service and also the security is attained.

REFERENCES

1 Basaran C, Kang KD. In: Misra S, Woungang I, Misra SC, Eds. Quality of Service in Wireless Sensor Networks. London: Springer 2009: 305-17.

2 E. Crawley, R. Nair, B. Rajagopalan and H. Sandick, 1998. A Framework for QoS-Based Routing in the Internet, RFC2386.

3 Sohrabi, K., Goa, J., Ailawadhi, V., and Pottie, G. J. 2000. Protocols for self-organization of a wireless sensor network. IEEE Personal Commun 7, 5 (Oct.), 16--27.

4 X. Huang and Y. Fang, "Multiconstrained QoS Mutlipath Routing in Wireless Sensor Networks," Wireless Networks, Vol. 14, No. 4, 2008, pp. 465-478.

5 D. C. Hoang, P. Yadav, R. Kumar and S. Panda, "Real-time implementation of a harmony search algorithm-based clustering protocol for energyefficient wireless sensor networks", IEEE transactions on Industrial Informatics, vol.10, no.1, pp.774–783, 2014.

6 J. Niu, L. Cheng, Y. Gu, L. Shu and S. K. Das, "R3E: Reliable reactive routing enhancement for wireless sensor networks", IEEE Transactions on Industrial Electronics, vol.10, no.1, pp.784–794, 2014.

7 P. Desnoyers, D. Ganesan, H. Li, and P. Shenoy, "Presto: A predictive storage architecture for sensor networks," in Proc. 10th HotOS, 2005.

8 M. Narasimha and G. Tsudik, "Authentication of outsourced databases using signature aggregation and chaining," in Proc. DASFAA, 2006.

9 K´alm´an Graffi, Parag S. Mogre, Matthias Hollick, and Ralf Steinmetz , "Detection of Colluding Misbehaving Nodes in Mobile Ad hoc and Wireless Mesh Networks," in IEEE GLOBECOM, November 2007.

10 Extended Watchdog Mechanism for Wireless Sensor Networks Lei Huang, Lixiang Liu, Journal of Information and Computing Science, 2007.

11 6-Youngho Cho and Gang Qu, Insider Threats against Trust Mechanism with Watchdog and Defending Approaches in Wireless Sensor Networks, IEEE Symposium on Security and Privacy Workshops, 2012.

12 Garcia-Macias, A., Rousseau, F., Berger-Sabbatel, G., Toumi, L., and Duda, A. Quality of service and mobility for the wireless internet. Wireless Networks 9, 4 (2003), 341–352.

13 Mahadevan, I., and Sivalingam, K. M. Quality of service architectures for wireless networks: Intserv and diffserv models. In ISPAN (1999), pp. 420–425.

14 Vali D, Paskalis S, Kaloxylos A, Merakos L. A survey of internet QoS signaling. IEEE Commun Surv Tutorials 2004; 6: 32-12.