

A Review on Transport Protocols in Wireless Sensor Networks

G. Raju ^{*1}, V. Ramesh ²

¹CSE Department, Assistant Professor, Vaagdevi Engineering College, Warangal, Telangana, India

²CSE Department, Assistant Professor, Sri Indu College of Engineering & Technology, Hyderabad, Telangana, India

ABSTRACT

The wireless sensor networks are a significant technological development into the various issues in several application areas associated with health, safety, environment, etc. This work focuses on sensor networks and in the main on the transport layer that should find and avoid congestion. It's desirable that the transport layers protocols offer responsibility suggestions planned solve issues of congestion and optimize energy. Many proposals are created for different transport protocols, typically oriented to optimize specific aspects and/or application scenarios. We did a study on wireless sensor networks and its varied transport mechanisms. We conjointly conducted a comparative study of many transport protocols. Thereafter, we emulated 2 transport protocols supported 2 main criteria that are reliability and congestion. We are very interested in the results to search out the most reliable protocol that has a transfer with the least loss.

Keywords : Wireless Sensor Networks, Transportation, Reliability and Congestion

I. INTRODUCTION

The transport protocols like transmission control protocol verified [2], designed to support user applications in infrastructure networks. One of the most factors for the failure of TCP is said to its reliability model strictly from setting out to finish, that forces all confirmations and retransmissions to follow the complete path between the supply and destination. Many suggestions are created for different transport protocols, typically oriented to optimize specific aspects and/or application [13] scenarios. Sensor networks are deployed from a wide extension of applications in military, agriculture, health, setting and therefore the field office. Determinant completely different characteristics counting on the application conditions like the kind of sensor data, the transmission rate, and responsibility. The protocols of the transport layer to the WSN or produce sensors surely applications is answerable for the operation of nodes in protocols within the network layer particularly in MAC [1] layers. In fact, their approaches don't appear applicable to all or any deployments of the device network. The transport layer needs many criteria like nonuniformity, responsibility, and manage congestion.

This PAPER, in its initial half, is an outline of transport protocols in WSN. Within the second half, we have a tendency to present a comparative study of those protocols taking into consideration 3 criteria are responsibility,

congestion control, and energy consumption. Then within the fourth part, we'll present an experimental study to hit a conclusion that shows the potential evolution of this work.

II. The transport protocols in the sensor network

The characteristics of sensor network, such as the dense deployment, the limited processing power and the limited power supply, provide design challenges at the transport layer. Care must be taken to design an efficient transport of layer protocol that combines reliability, heterogeneity and congestion control. The transport layer protocols in the sensor network allow communication between two layers transportation and then must be put in specific requirements [1] as follows: Credits: The protocol of the transport layer must be independent of applications, protocols for the network layer and the MAC layer, to be applicable for different deployments.

Support for heterogeneous data streams:

The protocol of the transport layer in the sensor network must be able to sustain a flow of

heterogeneous data. The two types of flow (continuous event_driven) must be present on the same network.

Reliability controlled variable: For some applications, the reliability must be complete while others can tolerate the loss of a few packets. In this case, the protocol of the transport layer must control this phenomenon and maintain energy in the nodes.

Detection and congestion control protocol must take into account the reduction in retransmission resulting in energy conservation packages.

Check the base station in the network:

Due to the computational capacity and the limited energy, most of the functionality must be performed in the base station.

Scalability: The protocol must be scalable (existence of a large number of nodes).

Accruals and future optimizations: The protocol must be able to adapt to future optimizations, to improve network operations and support for new applications.

2.1 STCP protocol

In computer networking, the Stream Control Transmission Protocol (SCTP) is a transport-layer protocol, serving in a similar role to the popular protocols TCP and UDP. It is standardized by IETF in RFC 4960.

SCTP provides some of the same service features of both UDP and TCP: it is message-oriented like UDP and ensures reliable, in-sequence transport of messages with congestion control like TCP; it differs from these in providing multi-homing and redundant paths to increase resilience and reliability.

In the absence of native SCTP support in operating systems it is possible to tunnel SCTP over UDP,[1] as well as mapping TCP API calls to SCTP ones.[2] The reference implementation was released as part of FreeBSD version 7. It has subsequently been widely ported.

Features of SCTP include:

Multihoming support in which one or both endpoints of a connection can consist of more than one IP address, enabling transparent fail-over between redundant network paths.

Delivery of chunks within independent streams eliminate unnecessary head-of-line blocking, as opposed to TCP byte-stream delivery.

Path selection and monitoring to select a primary data transmission path and test the connectivity of the transmission path.

Validation and acknowledgment mechanisms protect against flooding attacks and provide notification of duplicated or missing data chunks.

Improved error detection suitable for Ethernet jumbo frames.

The designers of SCTP originally intended it for the transport of telephony (Signaling System 7) over Internet Protocol, with the goal of duplicating some of the reliability attributes of the SS7 signaling network in IP. This IETF effort is known as SIGTRAN. In the meantime, other uses have been proposed, for example, the Diameter protocol[5] and Reliable server pooling (RSerPool).[6]

STCP protocol provides a paradigm for the transport layer, scalable and reliable sensor networks [1]. Most features of STCP are performed in the base station. Each node can be considered as a source of multiple data streams with different characteristics such as type of flow, the transmission rate and reliability required. STCP supports networks with multiple applications and causes additional features such as the control of the variation of the reliability and detection and congestion control.

2.2 The protocol PSFQ

PSFQ The protocol is designed to provide a number of segments from a single source node to a subset of receiving nodes, or all nodes in a sensor network. It guarantees delivery, for example, updates to the code.

The protocol consists of three basic primitives: an injection operation, a seek operation and an operation report. [2].

2.3 RMST protocol

The reliability in RMST refers to any subscriber, to all wells of all the fragments and some relating to a single entity RMST transfer. A single entity RMST is a data set consisting of one or more fragments from the same source. The order of transfer, which is not guaranteed,

is transparent to clients RMST. RMST does not include any guarantee in real time. There are two separate transport services to be added to the distribution: the effective management of the fragmentation and reassembly of the application based on semantic units and the guaranteed transfer [3].

2.4 CODA protocol

CODA is a congestion control technique that consists of three mechanisms for congestion detection: Open-loop, hop-by-hop backpressure and Closed-loop multi-source regulation. CODA attempts to detect congestion by regular monitoring of the transmission channel. If the channel occupancy exceeds a certain time interval, it implies that congestion has occurred. [4]

2.5 ESRT protocol

The Event-to-Sink Reliable Transport (ESRT) is a novel transport solution that seeks to achieve reliable event detection with minimum energy expenditure and solving congestion [7]. It aims at providing high reliability at providing between the sensors and the sink by congestion control [10]. The sink and the sensor nodes are not required by the protocol, to have a comprehensive knowledge such as the current number of available sensor nodes [8] [9].

2.6 GARUDA protocol

GARUDA belongs to the group downstream reliability guarantee. It addresses a similar problem as PSFQ, namely the reliable transfer of data block sink to the sensors or a significant part of the network. GARUDA uses a NACK-based arrangement. This solves the problem of NACK-based arrangements for receiving at least one packet of the block by detecting loss of other packets [8] [10] [11] [12] [20].

III. Comparative study of transport protocols

The main functions of transport control protocols for wireless sensor networks are: congestion control, ensuring reliability and energy efficiency. The existing protocols are studying congestion control or guarantee reliability in the way upstream (from the node to the sink) or downstream (towards the sink nodes). However, some applications in wireless sensor networks require both functions in both directions [15].

3.1 The reliability criteria

In this first part, we will mainly work on the reliability criterion. It is very important to provide support reliability at the level intermediate nodes which are more economic in energy than the treatment of end-to-end reliability. This is one reason why traditional mechanisms of TCP are not suitable (at least in the presence of unreliable links). Reliability criterion in the hop-by-hop model brings with it the problem of the security vulnerability of the transport layer, a problem that is rarely addressed in literature. While according to the end-to-end model, the intermediate nodes are expected to participate in the transportation of data by caching and retransmitting data packets, producing or modifying the contents of control packets (acknowledgments by example) to avoid end to end retransmissions. [13] There are some transport protocols such as STCP, ESRT, RMST examining upward reliability that is to say, the source node to the base station and others like PSFQ and GARUDA studying backward reliability (of the base station to the other nodes). [14] The ESRT protocol is concerned only with the reliability of event guaranteed by the adjusting rate of generated packets. However, RMST provides the reliability of packet loss recovery through one hop. The rate adjustment butt source in ESRT following two basic rules:

- If the current perceived reliability in wells exceeds the desired value, ESRT reduces the rate of source.
- Otherwise, the source rate is increased if the additive reliability required is not reached, unless there is congestion in the network.

Moreover, the protocols and STCP ART include mechanisms that can be used to provide reliability and differentiated based on the fraction of packets. ESRT estimates a single note of reliability for all traffic. Dynamic management levels of reliability and stable differential is still a research topic. PSFQ, GARUDA and ART are designed to provide reliable multicast downstream. ART is the only protocol that takes into account explicitly, both upstream and downstream of the reliable communication [13].

3.2 The criterion of congestion control In this second part, we will look at the congestion control. The congestion has a significant impact on the performance of reliable transport protocols. STCP is the only

transport protocol that supports both the reliability and congestion control. In addition, its congestion control but limits its reliability.

Almost all reliable transport protocols put control of disaster recovery at the receivers. ART may be an exception as regards to the transmission of ACK packets. The control at the receiver allows the continuous cleaning of the queues at the sender which increases throughput.

The RMST protocol jointly employs selective NACK and timer-driven mechanism for the detection and notification of loss.

Detection and explicit notification of loss meet the same problem of the implosion of control message. GARUDA and PSFQ use the NACK for loss detection and congestion, and local retransmission for the loss recovery, but they design different mechanisms to provide scalability [14].

While the second step is that the non-fundamental nodes recover the lost data of core nodes. GARUDA incites the reliability which study destination. However, PSFQ consists of three "operations»: injection operation, operation research, and report operations. In the injection process, the sink announces slowly and periodically the packets to its neighbors until all the pieces of data were sent. In the search operation, a sensor node enters the search mode once a sequence number space in a file fragment is detected. It also sends a NACK in the path reversed to recover the missing fragment. PSFQ does not propagate NACK messages to avoid implosion message.

Specifically, the NACK, received at an intermediate node will not be transmitted unless the number of NACKs that the node has received exceeds a predefined threshold and lost the requested segments by the NACK are unavailable at this node. PSFQ can be configured to use all the bandwidth and thereby overcome the delay caused by the slow injection [14]. GARUDA built a two-tier topology and suggests the restoring of loss at two levels. The two-level topology consists of two layers, respectively, for the cores of the non-core nodes and nodes [14].

The second problem of transport control protocols for wireless sensor networks is that it controls the

congestion by butt or hop by hop, although there is an end to end and hop by hop mechanism to the congestion control in the CODA; CODA uses these two mechanisms at the same time, and has no adaptive method to integrate the two mechanisms to achieve optimization.

3.3 The criterion of energy consumption Control strategy recovery of losses in the ART protocol receptors, increases the generation of ACK and NACK, which results in an increase in energy consumption. We must therefore assess whether the control of the sender loss or the control of the receiver is more suitable for a given WSN application. On the other hand, the adaptive congestion control that incorporates end to end and hop by hop may be more useful for WSNs with various applications, and useful for energy conservation and the simplification of the operation of the sensors [15].

3.4 Interpretation of the comparative study

Protocols discussed above consider the guarantees of reliability or the congestion control, except STCP, which examines both. Some protocols use the butt and others use the hop by hop to control congestion. Some protocols ensure reliability and provide other congestion detection packet. [14]. Sensor nodes in a WSN may have different priorities as they may be installed with different kinds of sensor and deployed in different geographic locations. Accordingly, the sensor nodes can produce sensory data with different characteristics. They may also have different priorities concerning the conditions of reliability and bandwidth. For example, most protocols of congestion control exige to sink to get the same output for all nodes. In addition, most reliable protocols use a simple identical to the loss recovery of loss for all the nodes and applications, except STCP. However, the nodes and the applications can consist of devices and diverse priorities that require a flexible loss recovery to optimize energy efficiency. [14] STCP is a protocol for transmission of ascending butt. It provides the reliability and congestion control, assigning the most responsibility sink. Intermediate nodes detect congestion based on the length of queue and inform the sink by placing a bit in packet headers [14]. This is a protocol for hop by hop open-loop congestion control for WSN, which objectives are to improve the output and energy conservation.

STCP uses the inter-arrival time of packet to estimate the degree of congestion. Unless the inter-arrival to be more precise, it may be due to excessive packet loss in the wireless environment. STCP also designs a simple mechanism to determine whether the received return signal must be relayed, however CODA employs degrees of congestion to run this. The increase is triggered by the sent signal back in STCP, but CODA, it is triggered periodically by the sensor node itself. CODA publishes the return signal when the buffer occupancy and / or channel charge beyond a threshold. It uses only the feedback signal to trigger the decrease in reduction rate sent. However, the feedback signal in STCP is used to adjust the transmission rate, including the reduction or increase [16].

IV. PROBLEM ANALYSIS

4.1 The choice of protocols

Among protocols considered in the transport layer, we chose to evaluate two. In our comparative study, the emulation protocols can be made according to two criteria: the congestion control and the reliability. However, it was noted that only the STCP protocol guarantee both the reliability and the congestion control. In addition, it is considered as the most recent protocol. Moreover, it was noted that the characteristics of protocol STCP closely resemble that of ESRT except that the latter is designed to control only the reliability. It was therefore decided to study these two protocols of reliability point of view and the congestion controls their implementations, emulation and the interpretation of results.

4.2 The emulation platform

There are many simulators for wireless networks. Especially for wireless sensor networks, found several simulators such as TinyOS, the OMNET + +, J-SIM, NS2 ... For the implementation of our protocols, we chose to use the emulator WSN, which has a simple interface and is implemented in Java language.

4.3 Experimental study

ESRT protocol operation and STCP is determined by the current state of the network, based on reliability and congestion state reached in the network. In this context, we have implemented these protocols on our platform

to study the relationship between the transmission rate and the standard reliability. This study will be shown in three curves representing three different scenarios for each protocol, ranging from one scenario to another the number of source nodes.

As already noted, the network of wireless sensors is characterized by its large number of nodes. In addition, our platform can not support a large number of nodes. So our emulation will be performed on a limited number of nodes (as the principle of operation of the network) and a base station that are randomly placed on the field of emulation.

To achieve our goal of emulation mentioned above, the implementation of our protocol emulation requires several parameters such as the required reliability (R), the decision interval (t), the number of packets sent (fn) and the number of received packets (r). The required reliability (R) is necessary for the calculation of the normalized reliability (η) = η knowing that r / R . In addition,

1. and (fn) are needed to calculate the rate of transmission (f) given that $f=fn/(n * t)$.

4.4 The implementation of the ESRT protocol

The algorithm works ESRT mainly on the base station. It is interested only in the collective information of sensor nodes within the event radius (Fig.1): whenever a sensor node detects an event, all its neighboring nodes placed in the event radius are required to transmit the same message detection base station.

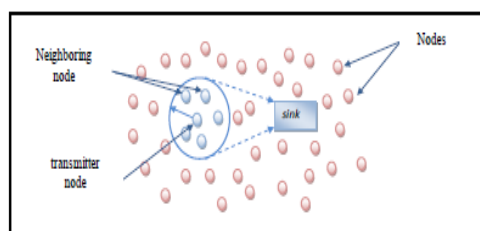


Figure 1: The topology of the sensor network

4.4.1 The first scenario Scenario1

As shown in Fig.2, our first scenario is as follows: an event is detected by the node (1). The field of transmission associated with this node (2) includes ten

nodes. These nodes are sources that will emit all the same event detected by (1) to the base station (3) nodes.

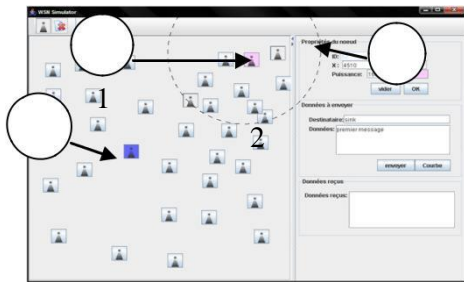


Figure 2 : The emulation scenario for ten knots source protocol ESRT

1. The node that detected the event (1)
2. Field of transmission (2): The source node and its neighbors who are concerned with the issue of the event to the base station
3. The base station (3)

V. Result

For the implementation of ESRT, the maximum number of packets (maxpaq) is an important parameter for congestion control: if the rate of packet transmission is strictly greater than the maximum transmission rate (fmax), then there is congestion.

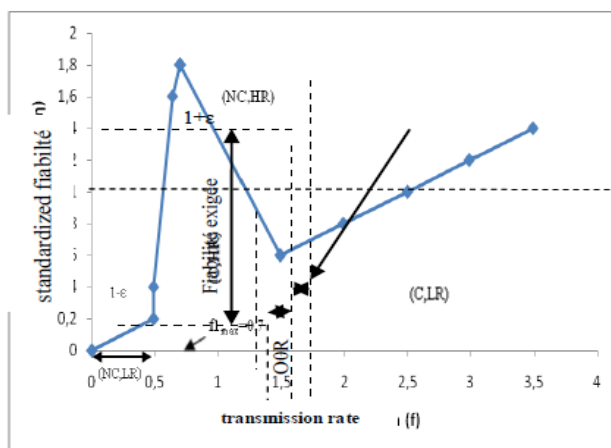


Figure 3

From this curve, we see that the maximum reliability (η_{1max}) 1.8 is reached. This maximum reliability requires a maximum rate of transmission $f_{1max} = 0.7$ packets / s. Identifying the f_{1max} , it is evident therefore also identify five areas of operation are ESRT protocol (NC , LR) , OOR , (NC , HR) , (C , HR) and (C , LR) .

- (NC, LR): In this region, the reliability standard (η) is between 0 and 0.4 therefore $\eta < 1 - \epsilon$ which implies a low reliability. In addition, the sending rate (f) is between 0 and 0.5 thus $f < f_{1max}$ where non congestion
- OOR: In this zone, f is between 0.5 and thus $0.64 f < f_{1max}$ standardized reliability and is between 0.5 and 1.5 therefore $1 - \epsilon \leq \eta \leq 1 + \epsilon$ where the problems.
- (NC, HR): According to the curve, this area is characterized by a f between 0.62 and $0.7 \leq f$ therefore f_{1max} therefore it is not congestion and η between 1.5 and 1.8 therefore $\eta > 1 + \epsilon$ and so is the high reliability
- (C, RH): On this area, f varies between 0.7 and 1.3 where $f \geq f_{1max}$ therefore is the case of congestion and $\eta > 1$ ranging from 1.8 to 0.9 where high reliability.
- ≤ (C , LR) : And finally, the standard in this area is reliability variation from 0.6 to 1.4 $1 - \epsilon \leq \eta \leq 1 + \epsilon$, so this is an area of low reliability and transmission rate is between 1.5 and 3.49 . As a result, it is also an area of congestion.

In areas of non congestion, the standard reliability is continuously growing. Soon as it reaches its maximum, it begins to decrease. This decrease is due to the congestion which automatically leads to a reduction of the standard reliability.

4.5 The implementation of STCP protocol

The principle of STCP protocol is to achieve a data transfer upon detection of an event by the sensitive sensors. Packet forwarding by a node is independent of other neighboring nodes. This transfer is triggered by a first of all initialization packet session (Session Initiation Packet). The latter is sent by a source node to a base station to open a session transfer indicating the packets to send. The principle of STCP protocol leads a base station to inform the sensor node with which it communicates the status of the transfer. This alert is made by a positive ACK if successful reception of the packet and negative acknowledgment NACK in case of error. We have simplified the operation of STCP protocol in Fig.9:

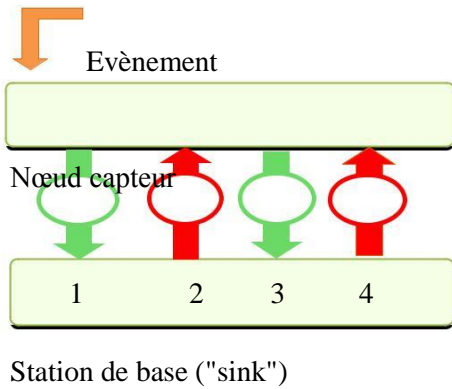


Figure 4: The reliability function of the transmission rate by varying the number of sources of ESRT protocol nodes

- In the event detection were:
- The sensor node sends a session initiation packet.
- The base station informs the node transfer status (ACK or NACK).
- If ACK:
- The node transmits its data packet.
- The base station confirms receipt with an ACK or failure by a NACK.
- If the NACK, the source node retransmits the same packet lost until it receives an ACK.

The exchange of data between a source node and a base station is done through the buffer at the source through the registry at destination. These devices work together to achieve a properly functioning STCP protocol using a timer.

For the experimental study of STCP protocol, we will test three scenarios by changing each time the number of source nodes.

4.5.1 The scenario Scenario

In this scenario, we used 10 source nodes and a base station ID. The noeu7 detects an event; it sends a data packet containing «test sending noeu7» to the base station. The message is displayed in the «data received» field with the ID of the source node. The exchange phenomenon data is initialized by sending the packet Session Initiation Package (SIP) and the transmission of its acknowledgment after sending data packets and their accused.

Initially, as shown in Fig.5, the registration of transfer by the source node (node1), the event detector, is shown by the color of the destination node in orange.

At this time, we are sure that the session initiation packet is transmitted.

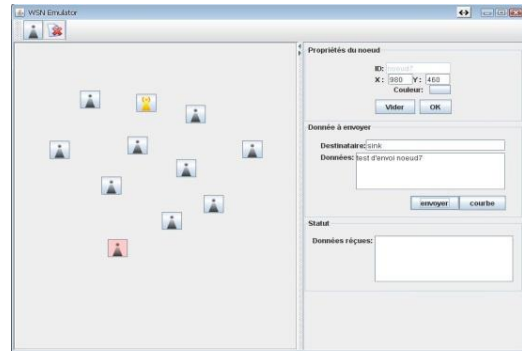


Figure 5: Sending Session Initiation Package source node to the destination node is the base station

Following receipt of the packet session initiation, the base station sending the accused to noeu7. Fig6 can present this action. The base station is now blue indicating successful reception of the packet session initiation.

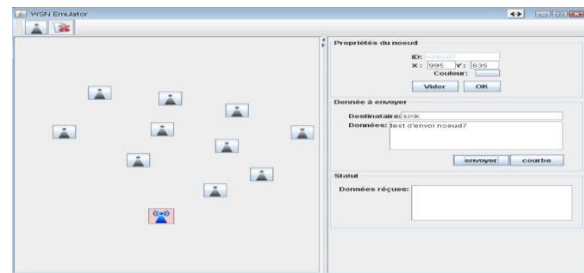


Figure 6. Transmission of an ACK packet session initiation of the base station to the nœud7

Upon receipt of ACK, the source node sends data packets. And the base station informs the source node (noeu7) state transfer. The emulation result STCP protocol for the first scenario is represented by the curve in Fig.13 which shows the variation of the normalized reliability depending on the transmission rate of packets.

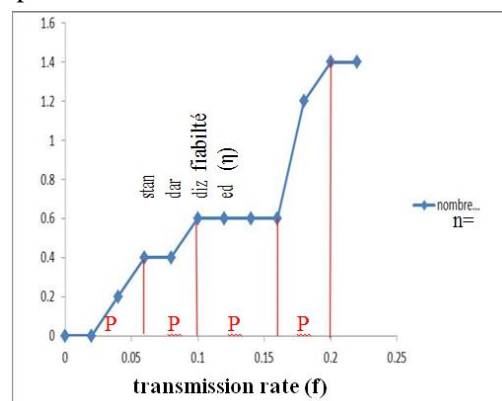


Figure 7 : Variation of normalized reliability function of sending packets rates tested with five knots sources STCP protocol

According to this curve, the standard growth rate of reliability based packet transmission continues. Indeed, if the sending rate increases over time increases, hence the speed increases gradually. This growth is due to the increase in nodes which leads to an increase in shipping rates. The algorithm STCP protocol controls reliability during transmission in order to ensure the smooth transfer. In fact, in the P1 part, we see a slight increase even it is zero at the beginning ([0-0.02]), which is explained by the fact that the beginning of sending packets of the produces a low reliability control because of the minimum number of packets. Then, the curve continues to grow slightly during the part P2. Whenever the rate of transmission increases the effective control of the reliability also augment to avoid any kind of congestion and of loss. In part P3, we observe a steady pace showing a state stabilization control standard reliability at a certain level of data transmission ([0.1-0.15]). We can deduce that there is congestion at excessive costs. It is for this reason that the curve maintains a constant level. As part P4, appearance has a significant improvement. The normalized reliability continues its development and the rate of data transmission increases. This result confirms the reliable transfer of STCP protocol.

This difference between the two curves is undeniable since the STCP guarantee reliability and congestion control at the same time, which explains the continued growth of its curve while the ESRT protocol does not guarantee the reliability, which explains the discontinuity of the curve which reaches its maximum reliability and as soon as it reaches the maximum transmission rate, it drops in reliability due to the congestion

VI. CONCLUSION

The wireless sensor networks are doubtless within the future to vary the method we live and work. They represent a significant technological development into the varied issues in several application areas, related to health, safety, environment, etc. In this paper, we've created a study of wireless detector networks and its numerous transport mechanisms. we've additionally conducted a comparative study of many transport

protocols. we tend to found that the prevailing transport protocols are dedicated either to ensure the responsibility or the congestion management in a very unidirectional direction (upstream or downstream). Some are designed to perform these 2 tasks at the same time, however in one direction and none of them is employed to attain them in each directions. However, some applications in detector networks while not son need each functions in each directions, the case of surveillance. Current researches during this area targeted on the conclusion of a reliable transfer with lowest loss of data taking into consideration the energy economy. It is, therefore, necessary to point out that the transport layer should do a decent transfer while not energy dissipation to prolong the lifetime of the detector, the most the maximum amount as possible. Indeed, the transport layer should be supported a new protocol for efficient and economical control of the transmission.

VII. REFERENCES

- [1]. Khenfouci Yamina and Badawi Amel "approach authentication in sensor networks for education," 2008/2009
- [2]. E. Feury David symplot-ryl "Sensor Networks", ISIC / INSA Lyon-ARES/INRIA, 16 December 2004.
- [3]. Claude Castelluccia, "Security sensors and sensor network."
- [4]. Badache, N. and T. Lemlouma. "The routing in mobile ad hoc networks." Research Report INRIA. 1999.
- [5]. Classification and comparison of routing protocols in wireless sensor networks, 2007/2008.
- [6]. I. Akyildiz, W. Su, E. Cayirci, Y. Sankara subramaniam. "A Survey on Sensor networks " , IEEE Communications Magazine , vol. 40 , no. 8, pp . 102-114 , Georgia Institute of Technology , Atlanta , USA. Aug. 2002
- [7]. B. Khalifa. " Security in wireless sensor networks " , lecture at the University of Bechar . Spring of 2006.
- [8]. Network - son without sensors. <http://www.techno-science.net>
- [9]. Yasser Romdhane " performance evaluation of S-MAC protocols and Directed Diffusion in sensor networks , project report at the end of study,

- Graduate School of Communications of Tunis, 2007.
- [10]. Sophia Kaplantzis " security models for wireless sensor networks ," research report, March 2006 .
- [11]. Bouabdellah Kechar " problem of energy consumption in wireless sensor networks son " LIUPA , University of Oran , October 2007 .
- [12]. Mohammad Ilyas , Imad Mahgoub , " Handbook of Sensor Networks : Compact Wireless and Wired Sensing Systems " , Chapter 15 , CRC Press LLC, 2005.
- [13]. Jamal N. Al- Karaki , Ahmed E.Kamal , " Routing in wireless sensors networks : a survey" , Dept.of electrical and computer engineering, Iowa State University.
- [14]. Sofiane MOAD , " Energy consumption in wireless sensor networks ," research study Master IFSIC - Rennes1 , 2007/2008
- [15]. jum zheng and abbas jamalipour " Wireless sensor networks : A Networking Perspective " .
- [16]. Severine Sentilles , "Software Architecture for wireless sensor networking son "master internet technologies , University Skin and Pays de l'Adour , in June 2006 .
- [17]. Lyes Khelladi , Najeeb Badache , " Sensor networks : state of the art " research report, USTHB , Algiers, February 2004 .
- [18]. Xavier Puga , "Introduction to sensor networks " , 2005 .
- [19]. LF . Akyildiz , W.Su , Y.Sankarasubramaniam , E.Cayirci , " Wireless sensor networks : a survey" , computer networks , vol 38, 2002.
- [20]. Claude Castelluccia and Aurélien Francillon , "protect sensor networks without son " , INRIA, 2008.
- [21]. http://fr.wikipedia.org/wiki/R%C3%A9seau_de_capteurs_sans_fil .
- [22]. Mehrotra, Shashank . " Distributed Algorithms for Tasking Large Sensor Networks. " Final thesis . 2001.
- [23]. Callaway, Edgar H. " Wireless sensor networks : Architectures and protocols . " CRC Press (2004).
- [24]. Savvides , A. , C.-C. Han and M. Srivastava . " Dynamic fine -grained localization in Ad- Hoc networks of sensors . " Mobile Computing and Networking (MobiCom) . ACM , 2001.
- [25]. Callaway, Edgar H. " Wireless sensor networks : Architectures and protocols . " CRC Press (2004).
- [26]. Mills , D. L. " Internet time synchronization : the network time protocol . . Global States and Time in Distributed Systems, " IEEE Computer Society Press (1994) : 1482-1493 .
- [27]. Karlof , C., N. Sastry and D. Wagner. " Tinysec a link layer security architecture for wireless sensor networks . " Reaserch article. 2004.
- [28]. Aboclaze , M. and F. Aloul . " Current and future trends in sensor networks : a. Survey" Wireless and Optical Communications Networks. IFIP International Conference , 2005. 551-555 .
- [29]. Chan , H., M. and A. Luk Perrig . "Using Clustering Information for sensor network localization . " Distributed Computing in Sensor Systems. Carnegie Mellon University, 2005.
- [30]. Ghiasi , S. , et al . " Optimal energy aware clustering in sensor . " Sensors (2002) :258-269 .109-125 .
- [31]. STCP : A Generic Transport Layer Protocol for Wireless Sensor Networks (Yogesh G. Iyer, Shashidhar Gandham , S. Venkatesan
- [32]. Data Transport Reliability in wireless Sensor Networks -A Survey of Issues and Solutions (Andreas Willig , Holger Karl)
- [33]. RMST : Reliable Data Transport in Sensor Networks 1 (Fred Stann , John Heidemann) T. Zhao , W. Cai, Y. and Li MPIDA : "A sensor network topology inference algorithm . ". In Proc. Int.Conf . on Computational Intelligence and Security , pages 451-455 , 2007.
- [34]. Y. Yang , Y. Xu , X. and Li Topology " tomography in wireless sensor networks based on data aggregation . InProc . " . Int . Conf . on Communications and Mobile Computing , pages 37-41 , 2009.
- [35]. Stefanos A " . Energy Efficient Routing in Wireless Sensor Networks Through Balanced Clustering " OPEN ACCESS Algorithm 2013