

Comparative Study of Transport Protocols in WSN

Ridha Azizi

High Institute of Technological Studies of Sousse (ISET),
Erriadh district - Sousse - 4032
Tunisia.

ABSTRACT

The wireless sensor networks are a major technological development into the various problems in many application areas related to health, safety, environment, etc. This work focuses on sensor networks and mainly on the transport layer which must detect and avoid congestion. It is desirable that the transport layers protocols provide reliability suggestions planned solve problems of congestion and optimize energy. Several proposals have been made for alternative transport protocols, generally oriented to optimize specific aspects and / or application scenarios.

We did a study on wireless sensor networks and its various transport mechanisms. We also conducted a comparative study between several transport protocols. Thereafter, we emulated two transport protocols based on two main criteria which are reliability and congestion. We are therefore interested in the results to find the most reliable protocol that provides a transfer with the least loss.

Keywords

WSN, transportation, reliability and congestion

1. INTRODUCTION

The transport protocols such as TCP proven [2], designed to support user applications in infrastructure networks. One of the main factors for the failure of TCP is related to its reliability model strictly from beginning to end, which forces all confirmations and retransmissions to follow the entire path between the source and destination. Several suggestions have been made for alternative transport protocols, generally oriented to optimize specific aspects and / or application [13] scenarios. Sensor networks are deployed from a wide extension of applications in military, agriculture, health, environment and the field office. Determining different characteristics depending on the application conditions such as the type of sensor data, the transmission rate and reliability. The protocols of the transport layer to the WNS or create sensors for certain applications is responsible for the operation of nodes in protocols in the network layer especially in MAC [1] layers. In fact, their approaches do not seem applicable to all deployments of sensor network. The transport layer requires several criteria such as heterogeneity, reliability and control congestion.

This document, in its first part, is an overview of transport protocols in WSN. In the second part, we present a comparative study between these protocols taking into account three criteria are reliability, congestion control and energy consumption. Then in the fourth part we will present an experimental study to arrive at a conclusion that shows the potential evolution of this work.

2. 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 Relevant Annotation Concept

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].

3. 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 butt 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 [13] 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 requires 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].

4. EXPERIMENTS

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.

The three scenarios are represented in the table below:

Table 1: Number of source nodes each scenario

Scénario	Number of source nodes (n)
Scénario 1	10 source nodes
Scénario 2	5 source nodes
Scénario 3	15 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, (t) 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.

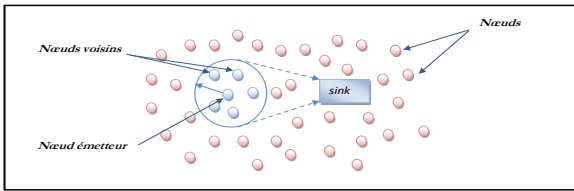


Fig 1: The topology of the sensor network

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.

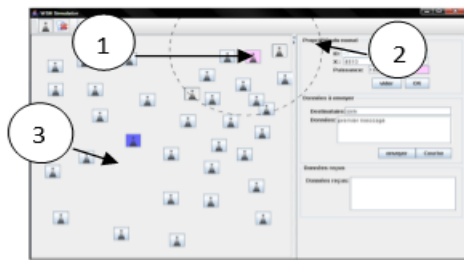


Fig 2: The emulation scenario for ten knots source protocol ESRT

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

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.

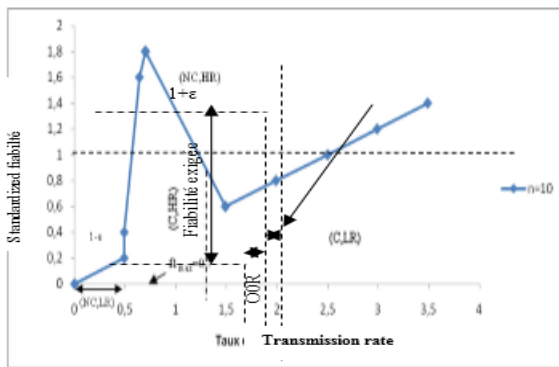


Fig 3: The result for ten knots source protocol ESRT

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.

4.4.2 The second scenario: scenario2

By reducing the number of source nodes, one obtains our second emulation scenario presented in Fig.4.

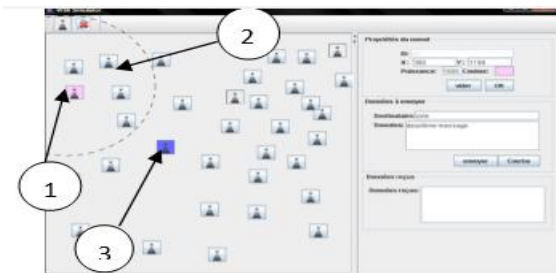


Fig 4: The emulation scenario for five source nodes protocol ESRT

This is the same principle as that of the first scenario, except that for this second scenario the transmission region contains only five nodes sources.

Result:

Keeping the same simulation parameters discussed above, the scenario of the second scenario allows us to get the result shown in Fig.5:

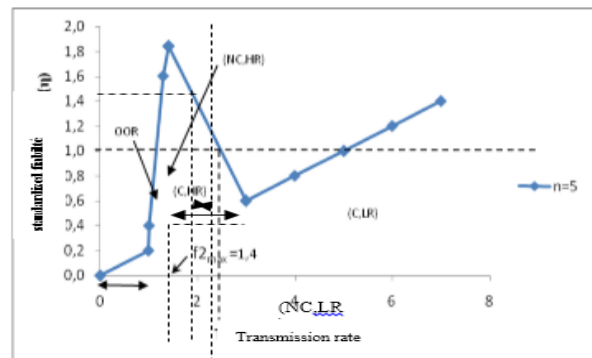


Fig 5: The result for five source nodes protocol ESRT

We note here the same pace of the previous curve but $\eta_{2max} = 1.8$ and $f_{2max} = 1.4$ packets / s.

- (NC, LR). For this region $\eta < 1 - \epsilon$ and varies between 0 and 0.4 so it's a low reliability In addition, the sending rate (f) is between 0 and 1 so $f < F_{2max}$ where non congestion
- REO: f in this zone is between 1 and 1.6 so $f < F_{2max}$ standardized reliability and is between 0.5 and 1.5 therefore $1 - \epsilon \leq \eta \leq 1 + \epsilon$ which implies the optimal operation.
- (NC, HR) : This zone is characterized by a f between 1.29 and 1.4 are therefore still in the case of $f \leq F_{2max}$ is therefore still not congestion and η between 1.6 and 1.8 therefore $\eta > 1 + \epsilon$ and so is the high reliability
- (C, RH) : By the way to the area, $f \geq F_{2max}$, the transmission rate varies between 1.4 and 2.5, therefore it is the case of congestion and η 1.8 starts to decrease towards 0,6 where high reliability.
- (C, LR): Regarding the latter area, the standard in this area is reliability variation from 0.6 to 1.4 so $1 - \epsilon \leq \eta \leq 1 + \epsilon$ and this area is of low reliability. The rate of transmission is between 1.5 and 3.49, so it also a congestion zone.

4.4.3 The third scenario: Scénario3

In this scenario we have also retained the same emulation settings but this time by increasing the number of source nodes to fifteen nodes as shown in Fig.6:

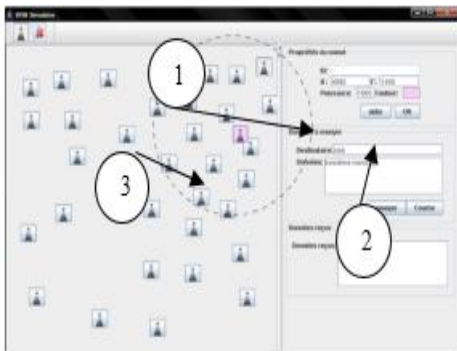


Fig 6: The emulation scenario for 15 knots sources ESRT protocol

Result:

As with the two previous scenarios, the result of our third scenario is illustrated in Fig.7:

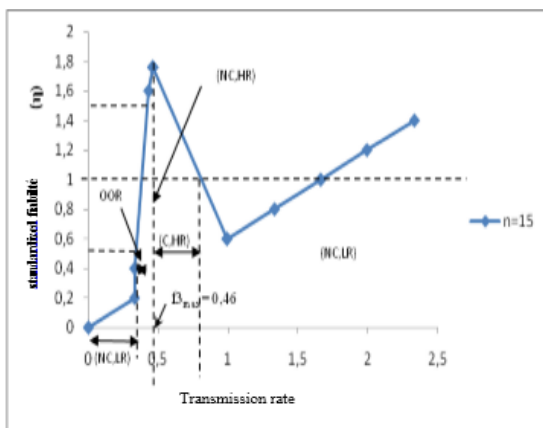


Fig 7: The result for fifteen knots source protocol ESRT

From this curve, the result of our third scenario is as follows:

The maximum standard reliability $\eta_{3max} = 1.8$ and the maximum transmission rate $f_{3max} = 0.46$ packets / s.

- (NC, LR). According to this curve, $\eta < 1 - \epsilon$ and varies between 0 and 0.4 so it's a low reliability In addition, the sending rate (f) is between 0.33 and therefore $f < F_{2max}$ where there is no congestion
- REO: For the curve f is between 0.33 and 0.43 so $f < f_{3max}$ for this region, η should be between $1 - \epsilon$ and $1 + \epsilon$ and therefore for our application should be between 0.5 and 1.5 and this is the case for our result.
- (NC, HR): This zone is characterized by a f between 0.43 and 0.46, therefore there is still in the case of $f \leq f_{3max}$ therefore it is still not the congestion and η between 1.6 and 1.8 therefore $\eta > 1 + \epsilon$ and so is the high reliability
- (C, RH): By the way to the area, $f \geq f_{3max}$, the transmission rate varies from 0.46 to 0.8 so it is the case of congestion and η 1.8 starts to decrease towards 0,6 where there is high reliability.
- (C, LR): Regarding the latter area, the standard in this area is reliability variation from 0.6 to 1.4 so $1 - \epsilon \leq \eta \leq 1 + \epsilon$ and this area is of low reliability. The transmission rate is between 0.8 and 2.33 and is therefore an area of high congestion.

4.5 Review of ESRT Protocol

To emphasize the difference obtained at f_{max} in the previous three scenarios, we superimposed the three curves on the same graph shown in Fig.8:

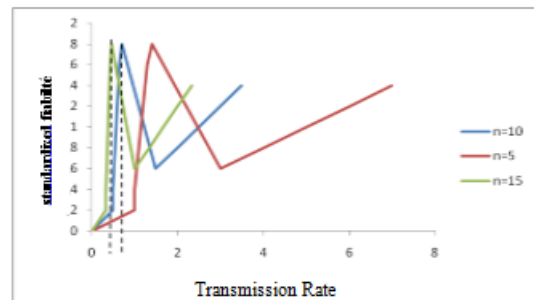


Fig 8: The reliability function of the transmission rate by varying the number of sources of ESRT protocol nodes

From this curve, it can be seen that the normalized maximum reliability is constant for the three curves. This result is obvious since we set the same reliability required (R) for the three scenarios and the same maximum transmission rate.

Regarding the transmission rate, there is a large change from one curve to another. This change also applies to the maximum transmission rate: we note here that $f_{3max} < f_{1max} < f_{2max}$. So in this sense we can conclude that the increase in number of sources nodes implies a decrease in the normalized reliability.

4.6 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:

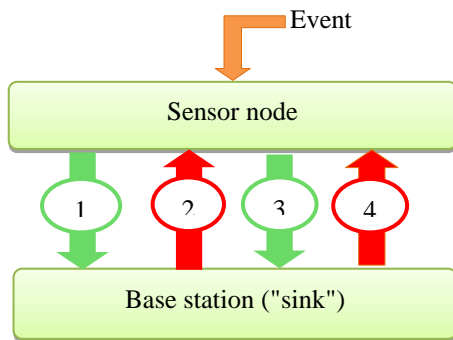


Fig 9: The reliability function of the transmission rate by varying the number of sources of ESRT protocol nodes

- 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.

4.6.1 The first scenario Scenario1

In this scenario, we used 10 source nodes and a base station ID. The noeud7 detects an event; it sends a data packet containing «test sending noeud7 »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.10, 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.

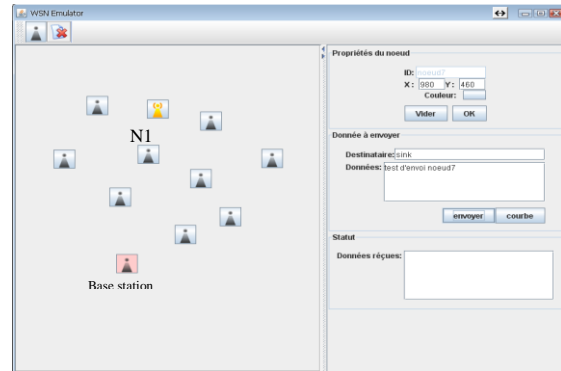


Fig 10: Sending Session Initiation Package source node to the destination node is the base station

- Following receipt of the packet session initiation, the base station sending the accused to noeud7. Fig.11 can present this action. The base station is now blue indicating successful reception of the packet session initiation.

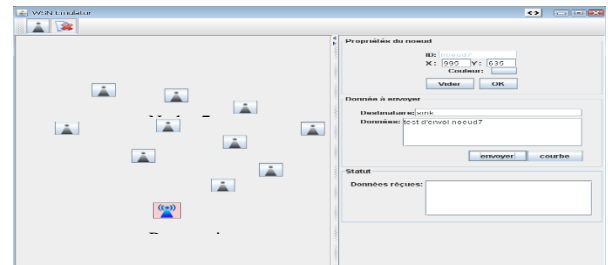


Fig 11: Transmission of an ACK packet session initiation of the base station to the noeud7

- Upon receipt of ACK, the source node sends data packets. And the base station informs the source node (noeud7) state transfer.
- If the transfer is successful is to say that the base station (sink) received data packets sent by the noeud7 while the latter will receive an ACK from the sink and it will be colored in green as shown in Fig.12.

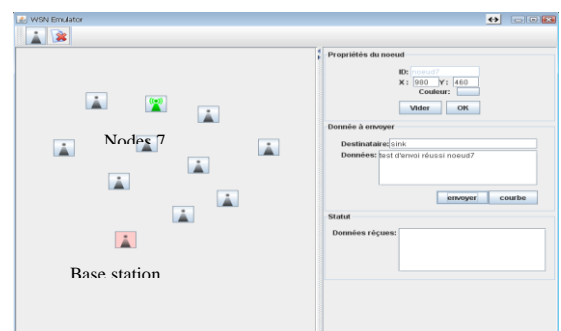


Fig 12: Receiving an ACK data by node1 from the base station

Result:

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.

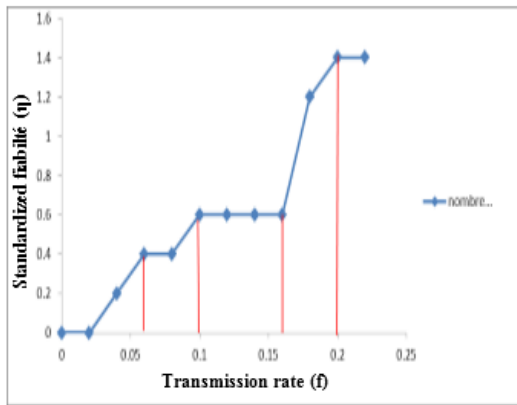


Fig 13: Variation of normalized reliability function of sending packets rates tested with five knots sources STCP protocol

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.

4.6.2 The second scenario: scenario2

In this scenario, we reduced the number of nodes compared to the previous scenario from ten to five nodes, and as a result we tested the transmission of node1 as Fig.14 shows:

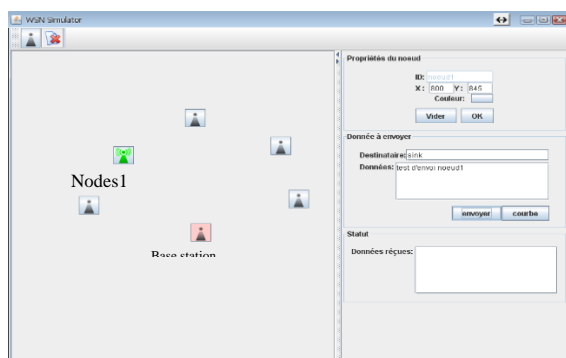


Fig 14: Reception of data packets by the base station node1

Result:

The emulation result STCP protocol for the second scenario occurs in the curve of Fig.15:

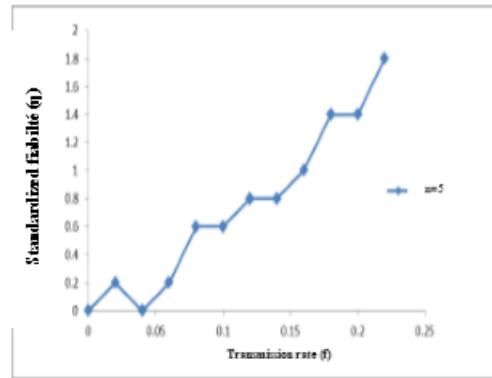


Fig 15: Variation of normalized reliability of packet forwarding rate tested with five sources of STCP protocol nodes

According to this curve, we see an increasing pace. Indeed, if the sending rate increases, the reliability standard also increases. STCP protocol guarantees the periodic exchange control data to reach the required reliability. The usefulness of ACK and NACK is to ensure the transmission of packets from source node to the base station. In fact, the transmission of data packets from one node successfully increases the number of received packets is the same number of ACK, which increases reliability of the standard. Otherwise, where the base station (sink) does not receive the transmitted data packet, it sends a NACK to the source node, it requests retransmission of the same packet which is destroyed or lost. Thus, the number of the packets sent will increase relatively to the number of received packets, hence the increase of the transmission rate.

4.6.3 The third scenario: Scénario3

In this scenario, we increased the number of node compared to the previous scenario from 10 to 15 knots, and as a result we tested the transmission of noeud12 and noeud15 and as shown in Fig.16.

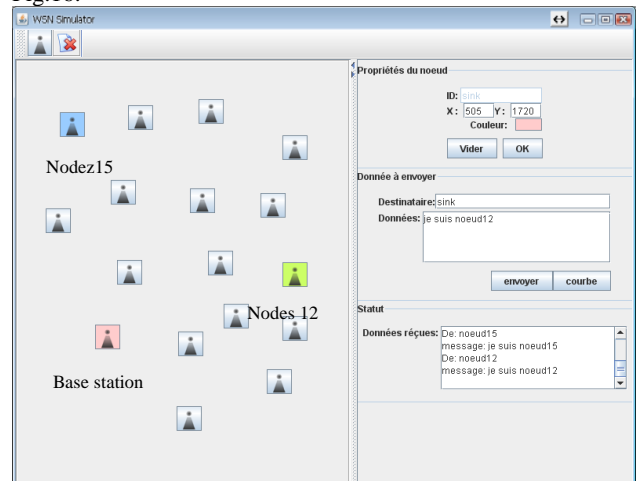


Fig 16: the reception of data packets by the base station of noeud12 and noeud15

Result:

The result shown in Fig.17 summarizes our simulation study STCP protocol using the third scenario.

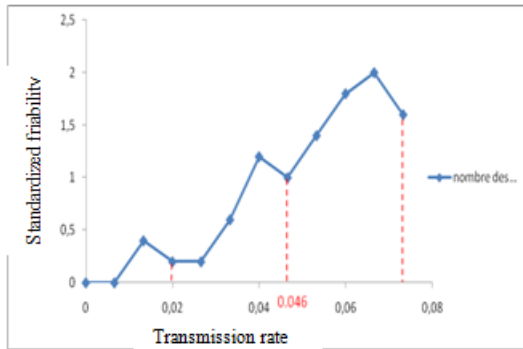


Fig 17: Variation of normalized reliability in terms of packet forwarding rate tested with 15 knots sources STCP protocol

In this curve, it can be seen the different variations of the standard as a function of the reliability of the transmission rate of packets. The normalized reliability increases rapidly as the sending rate increase slowly. Thus, we can deduce the significant influence of the number of source nodes on the rate of data transmission and the standard reliability. Indeed, this effect is to increase the rate of transfer of packets by the node detector, which causes the phenomenon of congestion. The appearance of the congestion produces failure cases of data loss cases. At this time, the principle of STCP protocol shows in controlling congestion which is represented by the sudden and temporary decrease of the normalized reliability at certain values of transmission rates (0,013 - 0.046-0.073).

4.7 Study of STCP Protocol

The emulation result STCP protocol for the three scenarios shown in Fig.18. Thus, we can deduce the effects and the influences of the variation of the number of nodes in the architecture network used in the course of the behavior of our STCP protocol.

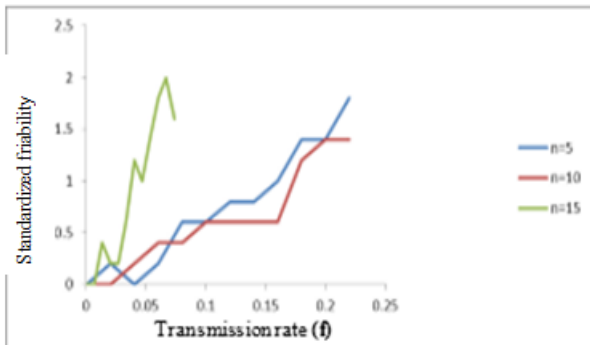


Fig 18: the variation of normalized reliability according to sending packets rates tested which three scenarios of STCP protocol rate

We notice that the differences between the three curves. The look in green, which is the study of the emulation of the first scenario, differs from other paces in a remarkable way. It has a large and rapid increase in the reliability standard (it reaches the value 2) according the rate of packet transmission. When using fifteen knots data sources, the transfer rate is necessarily excessive, or from the curve a small increase in shipping rates is noted. It is thanks to the congestion control, which regulates the rate of transmission to always achieve the expected level of reliability, we obtain a reliable transfer. Comparing this curve to the blue colored which has a node number equal to 5, there is a continuous and steady increase of two standards studied in parallel: reliability and congestion control. Tracing this rate is

explained by the low packet transmission in case there are five source nodes only. Thereafter, we notice that the curve plotted in red differs from the other two paces by the presence of a constant state of standardized reliability based on sending rate using ten nodes. This constant state implements the importance of STCP congestion control protocol that always seeks to achieve a good transfer under satisfactory reliability conditions. This improves the control of the sending rate for a reliable transfer.

5. SUMMARY OF THE TWO PROTOCOLS

To compare the two protocols, we superimposed in Fig.19, the two curves of the two protocols for n = 5:

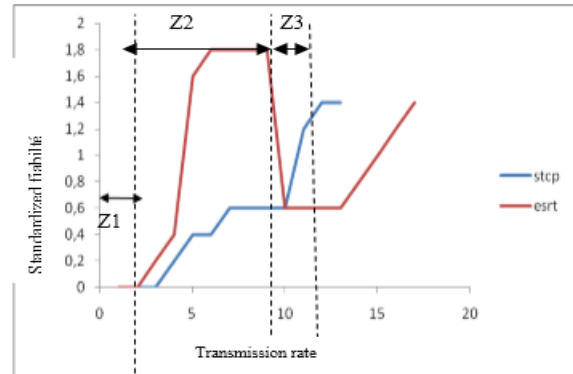


Fig 19: The synthesis of the two protocols and STCP ESRT five source nodes

From this figure, we see that for the first zone (Z1) the two curves are the same as for the second zone (Z2) we note that the ESRT protocol is much more reliable than the STCP protocol. Furthermore, for the third zone (Z3) it is found that the most reliable is STCP. We also note that the standard reliability STCP protocol is continuously growing while this is not the case for the ESRT 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.

6. CONCLUSION

The wireless sensor networks are likely in the future to change the way we live and work. They constitute a major technological development into the various problems in many application areas, related to health, safety, environment, etc.

In this paper, we have made a study of wireless sensor networks and its various transport mechanisms. We have also conducted a comparative study between several transport protocols. We found that the existing transport protocols are dedicated either to guarantee the reliability or the congestion control in a one-way direction (upstream or downstream). Some are designed to perform these two tasks simultaneously, but in one direction and none of them is used to achieve them in both directions. However, some applications in sensor networks without son require both functions in both directions, the case of surveillance.

Current researches in this area focused on the realization of a reliable transfer with minimal loss of data taking into account the energy economy. It is therefore necessary to show that the

transport layer must do a good transfer without energy dissipation to prolong the life of the sensor, the maximum as much as possible. Indeed, the transport layer must be based on a new protocol for efficient and economical control of transmission.

7. REFERENCES

- [1] Khenfouci Y and Badawi A "approach authentication in sensor networks for education," 2008/2009
- [2] Feury David symplot-ryl "Sensor Networks", ISIC INSA Lyon-ARES/INRIA, 16 December 2004.
- [3] Badache N. and Lemlouma T. "The routing in mobile ad hoc networks." Research Report INRIA. 1999.
- [4] Akyildiz E, Cayirci, Y. "A Survey on Sensor networks», IEEE Communications Magazine, vol. 40, no. 8, pp . 102-114, Georgia Institute of Technology,Atlanta, USA. Aug. 2002.
- [5] Khalifa B. «Security in wireless sensor networks ", lecture at the University of Bechar. Spring of 2006.
- [6] Yasser R" 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.
- [7] Sophia K "security models for wireless sensor networks", research report, March 2006.
- [8] Bouabdellah K "problem of energy consumption in wireless sensor networks son»LIUPA, University of Oran, October 2007.
- [9] Mohammad I, Imad M, "Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems.» Chapter 15, CRC Press LLC, 2005.
- [10] Sofiane M ,«Energy consumption in wireless sensor networks", research study Master IFSIC - Rennes1, 2007/2008.
- [11] jumzheng and abbasjamalipour "Wireless sensor networks: A Networking Perspective".
- [12] Séverine S, "Software Architecture for wireless sensor networking son» master internet technologies, University Skin and Pays de l'Adour , in June 2006 .
- [13] Lyes K, Najeeb B, "Sensor networks: state of the art " research report, USTHB, Algiers, February 2004.
- [14] Xavier P, "Introduction to sensor networks ", 2005.
- [15] Claude C and Aurélien F , "protect sensor networks without son ", INRIA, 2008.
- [16] Mehrotra, S. «Distributed Algorithms for Tasking Large Sensor Networks.» Final thesis. 2001.
- [17] Callaway, Edgar H. "Wireless sensor networks: Architectures and protocols". CRC Press (2004).
- [18] 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.
- [19] Callaway, Edgar H. "Wireless sensor networks: Architectures and protocols. »CRC Press(2004).
- [20] Mills, D. L. "Internet time synchronization: the network time protocol. Global States and Time in Distributed Systems, " IEEE Computer Society Press 1994 : 1482-1493.
- [21] Karlof, C., N. Sastry and Wagner B.. «Tinysecalnk layer security architecture for wireless sensor networks. »Reaserch article. 2004.
- [22] Aboclaze, M. and Aloul F. «Current and future trends in sensor networks: a. Survey" Wireless and Optical Communications Networks. IFIP International Conference, 2005. 551-555.
- [23] Chan, H., M. and LukPerrig A. "Using Clustering Information for sensor network localization.» Distributed Computing in Sensor Systems. Carnegie Mellon University, 2005.
- [24] Ghiasi, S., et al. «Optimal energy aware clustering in sensor. » Sensors (2002):258-269 .109-125.
- [25] Data Transport Reliability in wireless Sensor Networks -A Survey of Issues and Solutions (AndreasWillig,HolgerKarl)
- [26] RMST : Reliable Data Transport in Sensor
- [27] 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.
- [28] 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.
- [29] Stefanos A. "Energy Efficient Routing in Wireless Sensor Networks through Balanced Clustering" OPEN ACCESS Algorithm 2013.