A New Proposal for Trust Management in Wireless Sensor Networks based on Validation

Albert Rego, Christos Gkountis, Laura García, Jaime Lloret

Integrated Management Coastal Research Institute, Universidad Politecnica de Valencia,
C/ Paranimf nº 1, Grao de Gandía – Gandía, Valencia (Spain)

Emails: alremae@teleco.upv.es, cgkountis@hotmail.com, laugarg2@teleco.upv.es, jlloret@dcom.upv.es

Abstract: Due to their many advantages, WSNs are getting more and more important in the field of monitoring and control systems. Despite their many advantages WSNs have some disadvantages that need to be solved. Trust-based networking can be applied to WSNs in order to get better their performance. In this paper, we proposed a new model for trust management between sensor nodes in a WSN based on false alarms they produced. The existence of validators in the WSN supports the node to determine if the alarm is a false positive. A communication model is proposed and its messages are described. Furthermore, we have performed several tests to validate the benefits of our proposal, measuring the energy consumed by the network and each individual node in the network in five scenarios. They showed us that not trusting all of the nodes in a WSN, can have better results in the total energy consumption of the network. However, having a high number of malicious nodes causes an increment of energy consumption in the rest of the nodes.

Keywords: validation; wireless sensor networks; alert detection system; fire detection; trust management; proposal; simulation.

Reference to this paper should be made as follows: Author. (xxxx) ‘Title’, *Int. J. xxxxxxxxxxx xxxxxxxxxxx,*

1 Introduction

The damage caused by forest fires is incalculable. The damage created by them affect both the people and the environment. Areas of the world with high temperatures and little rain are more prone to suffer from this kind of natural disasters. Also, many times fires are started by people, either willingly or as a negligence. From the figures provided by the Ministry of Agriculture, Alimentation and Environment of Spain, in 2015 11.928 incidents were registered, with a total of 103.199,96 hectares of forest areas affected (Ministry of

Agriculture, Alimentation and Environment of Spain, 2016). Apart from the loss of forest areas, fires can cause housing damages and even cause people's death. In order to avoid the consequences of a fire or to minimize its damage, fire detection systems were created.

Nowadays there are many fire detecting solutions based on Wireless Sensor Networks (WSN). These networks are composed of a great quantity of sensor nodes that gather the desired data and communicate with each other. Sensor nodes can be placed in the exact spot where the event is happening or close to it (Akyildiz Ian F et al, 2002). These nodes can perform simple computations in order to forward the information partially processed. Its applications are not only related to environmental purposes. WSNs can be deployed for military, health and home applications as well.

Due to the large number of sensors employed in WSNs, sensor failures are a problem to consider (Muhammad Adeel M. et al, 2015), such as problems derived from the transmission of the data (Dulman S. et al, 2003), or failures at gathering or processing the data. These failures in WSNs can cause problem such as not being able to detect or predict a fire, along with its consequences, as well as forwarding an emergency alert when there is no fire or the possibility of it, which can involve a great cost of money from deploying the firefighter troops and their equipment.

In this study, we propose a fire detecting system that uses cameras to verify whether the alarm is true or not, so as to avoid the deployment of the relevant forces in unnecessary cases. The information gathered on false positives is stored and processed. With the obtained data, a trust system is created where each node is categorized by their reliability. If the data gathered by a sensor node is always correct, the reliability level will be maximum. If the data is not always true, the system will not always trust the alerts originated from that node. If the information originated by a node is mostly untrustworthy, the system may stop listening to the alerts raised by that node during a certain period of time.

The rest of the article is structured as follows. In section 2, the related work on fire detecting systems using WSN and the reliability of WSNs is described. A general description about the model and the networks where is planned to use in is made in section 3. An example of working is used to explain the remaining details of the system in section 4. In section 5 the simulations done and the results obtained are discussed. Finally, in section 6 the conclusions are shown and the future work from this proposal is commented.

2 Related Work

Throughout the years, several fire detection systems using WSN have been designed. Jaime Lloret et al. propose (Lloret J. et al, 2009) a fire detecting system that uses WSN and IP cameras to verify the existence of fire from the point of view of wireless signal and traffic generated from the cameras. When the fire is detected, a multisensory network forwards an alarm to the central server. Then, the cameras that are closest to the sensor that raised the alarm, point towards it in order to provide the images of what is happening in the area to the firefighters. They also study the energy consumption of the devices.

Liyang Yu et al. propose (YU L. et al, 2005) a fire detection method using a great quantity of deployed sensor nodes that collect data on the weather. The gathered data is used to predict the probability of a fire caused by the weather conditions. If any sensor detects smoke or high temperature, an emergency report is forwarded to the manager node. They classify the data into Regular Reports, Query Responses and Emergency Reports in order to stablish a priority in handling the data.

Anamika Chauban et al. use artificial neural networks to classify the data obtained by the sensors (Chauhan A. et al, 2013). To transmit the data wirelessly they use BTBee. In case of emergency, an Emergency report with more priority is forwarded. They use a Support Vector Machine to classify each type of data.

A WSN fire detection system that can increase its alarm accuracy utilizing several attributes to make the decision is presented by Liu Yo et al. (Liu Yo. et al, 2011). To implement the detection using multiple criteria, they employ artificial neural networks, which provides low overhead and a self-learning functionality. The prototype has been built using TelosB sensor nodes. They also have developed a solar battery that allows the nodes that are placed in areas with few sunlight to charge.

The use of these systems is of great help to prevent and act against fires, but the alarms raised by the sensors of the WSN may not be true. Because of that, some studies on their reliability have been done. Anton Herutomo et al. perform a reliability test of a fire detection system employing OpenMTC (Herutomo A. et al, 2015). The utilized WSN is called Zigbee. In their study, they conclude that the accuracy of the detection depends on the type of sensor used, its placement and the gateway placement, in order to be able to connect with it via Internet in remote areas. Al-Abassy Y. et al. measure the reliability of three fire detection MAC protocols that were proposed in their previous works (Al-Abbasss Y. et al, 2011). These protocols are called Persistence CSMA/CA, Per Hop Synchronization and Sensor TDMA. They propose a reliability enhance mechanism that has a small increase in energy consumption compared to the performance without the employment of said mechanism.

Studies on the overall reliability of WSNs have also been done. Trust systems for WSNs have a similar purpose but their implementation may vary in accordance to the approach followed by their creators. Avinash Srinivasan et al. present a reputation-based trust model for WSN, called DRBTS (Srinivasan A. et al, 2006). In this model, each Beacon Node monitors its neighbours to detect misbehaving. The results are uploaded in a Neighbour Reputation Table. The obtained information is used to decide if the information gathered by a node is trustworthy and thus, acceptable for its use. Another reputation-based model is presented in (Piero Bonatti et al, 2007). They determine that a trust management system should not be based only on a reputation-based model. An integrated method that employs a rule-based and a credential-based approach is proposed in order to provide a trust management framework that is able to operate in a wide range of scenarios.

Xiaoyung Li et al. propose a WSN trust system based on clustering algorithms (Li X. et al, 2013). They improve the efficiency of the system eliminating the feedback between cluster members and between cluster heads. They also propose a self-adaptive weighting method for the trust aggregations of the cluster heads. Riaz Ahmed Sahikh et al. propose another system that utilizes clustering (Riaz Ahmed Sahikh et al, 2009). The cost of the assessment of the level of trustworthiness of a node is minimized and the memory employed in performing those calculations is reduced. The proposed system uses less communication overhead and protects against untrustworthy nodes. They proposed a hybrid group-based management system in (Riaz Ahmed Sahikh et al, 2006) where the nodes classified other nodes as trusted, un-certain and un-trusted, and forwarded the information to the base station. Then, the base station multicasts the information to all the nodes. Another clustering-based system is proposed in (Febye Bao et al, 2012) where they use both subjective and objective test to evaluate the performance of their proposal. An optimal threshold level is found in order to reduce the cases of false positives and negatives.

Ninghui Li et al present a role-bsaed trust management system that employs attributes from attribute-based access control systems, role-based access control systems and SDSI (Simple Distributed Security Infrastructure) (Ninghui Li et al, 2002).

Throughout the years, several surveys on trust management systems for Wireless Sensor Networks have been done. Guanjie Han et al. compare several trust models differentiating whether they are based on nodes or on data (Guanjie Han et al, 2013). To do so, they evaluate for each solution the methodology it employs, the trust values, the advantages and limitations and the complexity of the model. They also compare the resiliency of each model based on the attacks they can handle successfully. In (Theodore Zahariadis et al, 2010) the authors evaluate the implementation requirements, the consumption of resources and the level each of them has achieved. In (Javier Lopez et al, 2010) a list of best practices for deploying trust management systems in WSNs is presented. An evaluation of the existing systems on whether they implement these practices or not is performed as well. In (Stephen Weeks, 2001) a mathematical framework of trust systems is presented. It was developed in order to facilitate the comprehension of the performance of trust systems.

In our proposal, we present a trust system for fire detection using WSN. To do so, several cameras verify whether the alarm has been raised because of a real emergency or not. With the obtained data on false positive alarms the system decides the trustworthy level of a node. If the trustworthy level decreases substantially, the system may decide not to act on the information received by that node for a period of time.

3 Network Model and Description

The system designed and the main working diagrams are described in this section. Firstly, how the model works is descripted.

3.1 General Model Description

This section describes a model to manage trust inside a wireless sensor network that is being used to detect some alert, e.g., fire in a farm or in a park.

The wireless sensor network that uses the model presented in order to manage which nodes are trustable or not is composed by two elements; the common sensor which make their measurements and communicate between them and validators like cameras. The main idea of this model is to use the validators in order to determinate when a sensor is sending a false alarm either when it is wrong/broken or it is a malicious node. A graphical example is shown in Fig. 1, where a network with nodes (blue points) and validators (brown points) can be seen. Furthermore, one node with communication with either actuators or some entity or server in the outside is needed. This node is referenced as gateway from now on.

The model presented can be divided into three parts. In the first place, the nodes use a protocol for discovering their neighbours and create the network. In order to do this, they connect with their neighbours using Wi-Fi and a session WEP key. This is done in the Media Access Control layer. In the above layers, the user is identified either on the Network layer or in the Application layer. This decision is not discussed in the paper. In the next sections, we assume that the nodes have an identifier and it is possible to address them. However, in terms of security, using an identifier in the application layer is better.

The next part is the communication module. This model section describes the messages that the nodes send and receive during the communication. A resume of all the messages is shown in Table the messages exchanged between the nodes 1 are classified attending to the level of alert that is graphically shown in Fig. 2. The messages that allows nodes joining to the network have not been detailed in Table 1 because in this paper the first part of the proposal is not detailed.

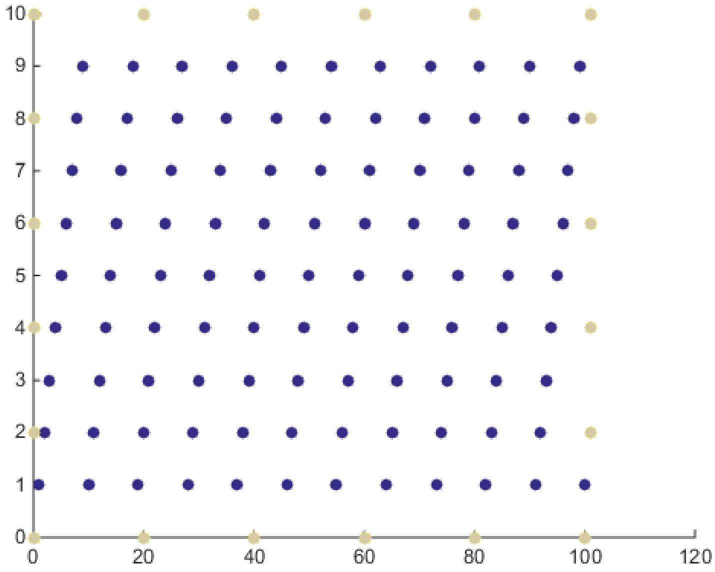

Fig. 1. Graphic distribution example.

Destination	Classification	Message	Description
Node	Maintenance Message	ACK	Confirms that the previous message has been successfully received.
Node	Maintenance Message	Routing	Messages related to routing protocol (Not detailed)
Node	Maintenance Message	Status Request	Allow a node know if its neighbour is disabled or not.
Node	Maintenance Message	Enabled Node Report	Indicates that the node is enabled.
Node	Maintenance Message	Disabled Node Report	Indicates that the node is disabled.
Node	Data Communication	Data Request	Allows a node request some data to its neighbours.
Node	Data Communication	Send Data	A data package response.
Node	Level 3	Disabling Node	Allows a node disabling an untrusted neighbour.
Node	Level 3	Critical Situation	It can be used to report an unusual situation.
Node	Alert	Alert	Reports an alert detected by that node.
Node	Alert	Alert Forwarded	Reports an alert that has been reported from another node.
Validator	Validator	Validate Area	Request a validation to confirm an alert.
Node (From a Validator)	Validator	Alert	Confirms a true alert situation.
Node (From a Validator)	Validator	False Positive	Discard an alert claiming that has been a false positive.

Table 1. List of Messages.

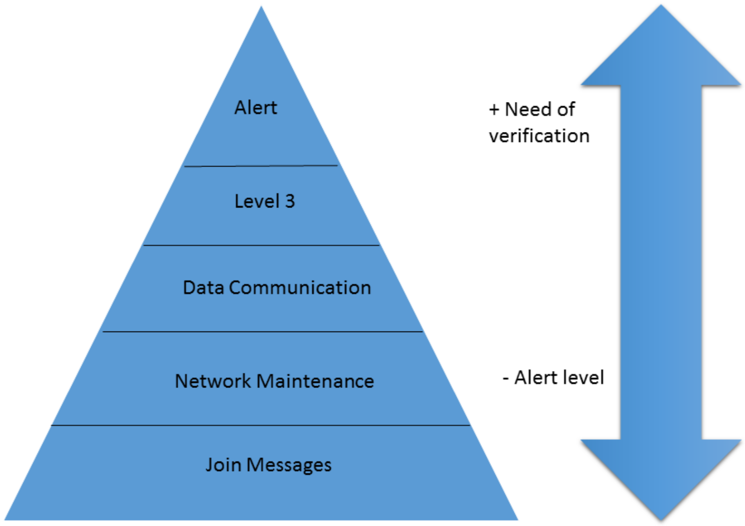

Fig. 2. Internode Message Classification.

The last part of the model is the management of which nodes are trustable and which ones not. This part is done based on a black list. At the beginning, all the nodes trust in each other. Along the lifecycle of the system, the nodes may add their neighbours into the untrusted nodes list. The decision of adding a node in the list is based on the false positive that node send. Attending to the Table 1, when an alert message is sent from a node n to their neighbours, the first neighbour in the path and the gateway can verify with the validator, e. g. a camera, if the alert is really true. If the validator, which has to have a major success rate, does not detect an alert situation, the node will mark these messages as a false positive. Depending of the implementation, the node would count until a fixed number of false positives before adding the sender as an untrusted node. Once a node adds a neighbour to the untrusted nodes list, it sends a message to the neighbour informing it in order to avoid unnecessary communication in a period of time and so reduce the energy consumption. If some neighbour establishes a communication with a disabled node it will be reported that that node is disabled until a specific time. This is done because, in the period of time the node is marked as an untrusted node, its neighbour will not listen to the messages coming from it. Therefore, the node will not consume energy from communication in this period of time. Additionally, it is possible that the disabled node was in the active path of communication with the gateway. If some previous node in the path communicates with the disabled node, it will be reported with a Disabled Node Report message and the path will be recalculated using the routing protocol.

The nodes need a data structure that implements the untrusted node list in order to manage not only which nodes are untrusted but to manage also the false positives given from every neighbour and the time when these nodes are removed from the list.

3.2 Additional proposed to improve the model

Some variations or optional proposals that can be added to the system are explained in this subsection. First of all, the model proposes an alternative to the total disabling of an untrusted node. In the model, when a node becomes untrusted from the point of view of some neighbour, the untrusted node is reported by its neighbour in order to reduce the energy consumption. In non-dense sensor networks, disabling nodes may cause loss of connectivity between the nodes. As an alternative, in scenarios where the probability that the source of the false positives was a malicious node was low, an only-forward message can be sent instead of the disabling message. In that case, the untrusted nodes will not stop to communicate with their neighbours, but they only forward the alert messages originated in another node. This option increases the network connectivity, avoiding recalculating the routing path but increasing the energy consumption in the untrusted nodes.

Additionally, the nodes may trust in their neighbours attending to a classification based on previous false positive or previous succeeded communications. During the working of the system, a node can increase how much it trusts in their neighbours. If one node has enough trust in its neighbour it may not add it to the untrusted nodes list when a false positive is sent by it. However, to do this classification, the nodes need another list with their neighbours. In the next section, besides the normal working of the messages exchanged and general working, this trust graduation is detailed and how a node can be more trustable is described.

4 Description of a Study Case

In this section, the usual working of the system is described using an example. First of all, we assume we have a wireless sensor network like the one in the Fig. 1. This network has been created by the discovering protocol using Wi-Fi and a WEP key.

Once the network has been created, all the nodes have an empty untrusted nodes list. Furthermore, in this example we are going to consider that nodes classify their trust in the other nodes. In that case, they use a neighbour list in order to know in every moment the trust they have in their neighbours. Fig. 3 shows the node state diagram, where how to change the trust with the other nodes is detailed. At the beginning, a node that establishes communication with a neighbour starts at the first state. In this state, its neighbour has the minimum value of trust in it. With the normal message exchange, level 1 and level 2 messages, the node may pass into the second state. It can pass also with a valid alert detection message, either forwarded or originated in its area. A node that is in the second state is a node whose neighbour has exchanged several succeed messages with it. It has not enough trust in this node to considerate that it is not a malicious node. When these nodes promote into the third state sending a valid alert detection message, the neighbour has enough trust in it to not add it into the untrusted nodes list when a false positive is sent.

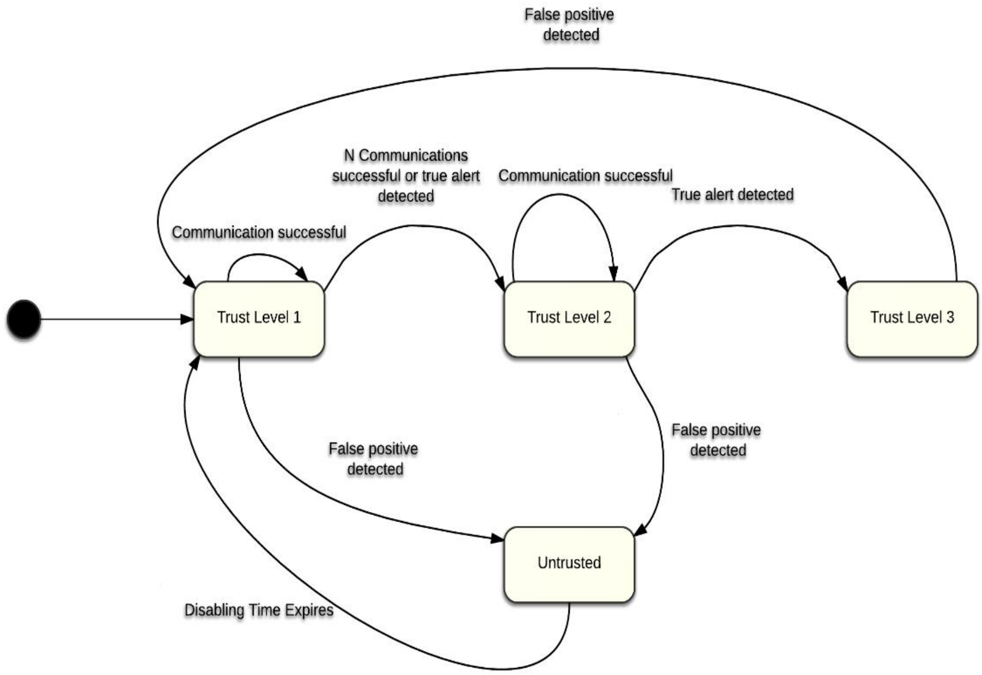

Fig. 3. State Diagram.

In our example, we are going to show the usual working of a couple of nodes. Given any pair of neighbour nodes (node A and node B), they have an empty untrusted nodes list and a neighbour list in which both of them have the other node. During their working, they send each other messages like those in the Fig. 4. This communication continues until one of them, maybe both of them, promote its neighbour to the second trust grade and indicate it in the list. From this moment, an alert situation occurs and node A sends an alert message to alert B. Two different scenarios are going to be described. In the first of them, the alert is a false positive. On the other hand, the alert is a true emergency situation. Fig. 5 shows the communication between node B and the validator related to the first scenario meanwhile Fig. 6 is related to the second one. Both communications are very similar, the only thing that changes is the answer from the validator.

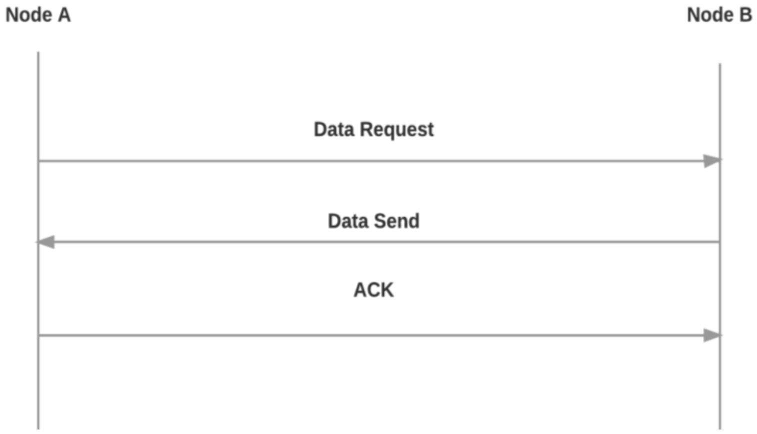

Fig. 4. Usual Data messages exchange.

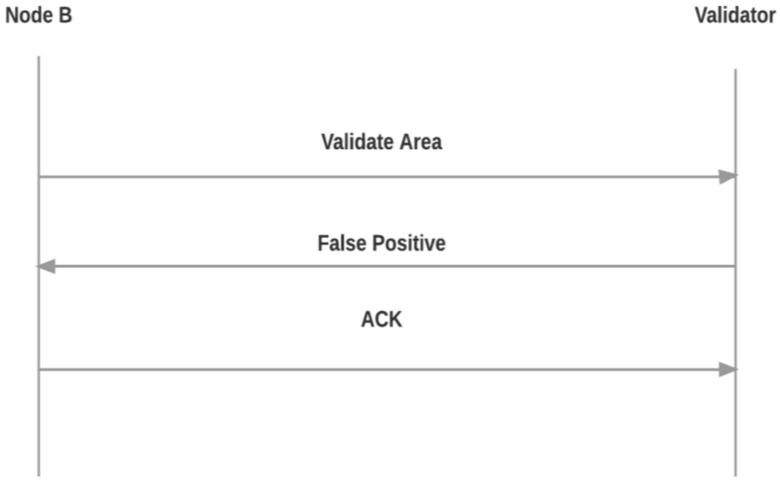

Fig. 5. Messages exchanged during a false positive detection by the Validator.

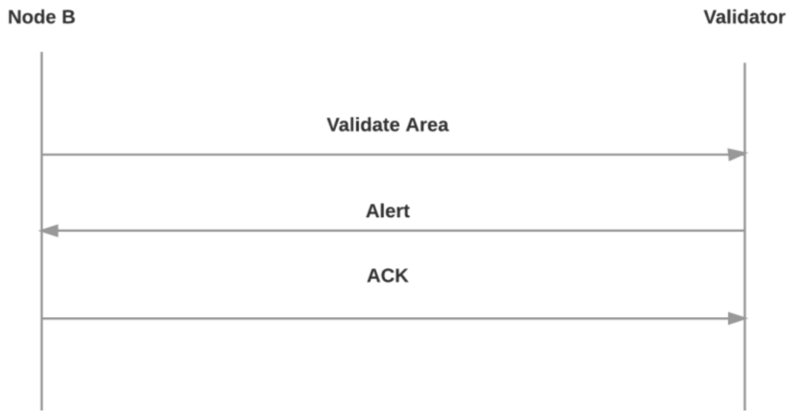

Fig. 6. Messages exchanged during a validation.

Attending to the second scenario, node B promotes node A to the third state, where a false positive would send node A into the first state again and, from the point of view of B, it would be again at the beginning.

However, the most interesting scenario is the first one, where a false positive is sent and node B stops relaying on node A. In this moment, a communication like Fig. 7 is established and node B adds node A into its untrusted nodes list. The entry has an expiration time that is set by node B and it is communicated to node A in the communication shown in Fig. 7, specifically in the Disabling Node Message. If there is a malicious node that sends Disabling Node messages, its neighbor will not send the Disabled Node Report, but adds these nodes into untrusted nodes list cause in the usual working one node only sends that message when an alert is validated. Therefore, that malicious node will be isolated.

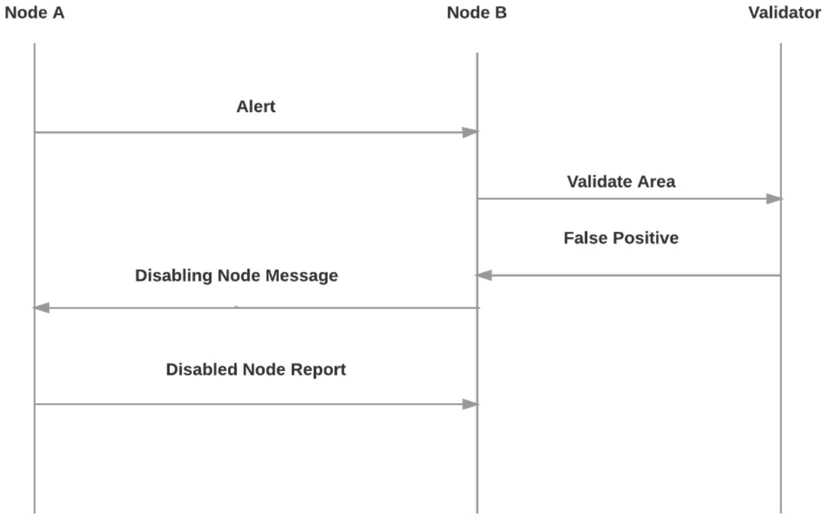

Fig. 7. Messages exchanged during a node disabling.

In this time interval, another node, node C, wants to send data to the gateway, and node A is the next hop in the path. Node A sends a Disabled Node Report message with the expiration time set by node B. Node C adds Node A to its untrusted node list and runs the routing protocol in order to recalculate the path. When expiration time is reached, Node C may recalculate the routing path depending on how much the new route is worse than the original one. Before that, it has to send a Status Request in order to check if Node A is still disabled. If Node A is disabled, it will send a Disabled Node Report. Otherwise, it will send an Enabled Node Report.

When Node A is enabled again, it sends an Enabled Node Report to Node B. Node B removes Node A from its untrusted nodes list and returns it to the first state.

Finally, in Fig. 8 the entire communication between the nodes of the network is detailed.

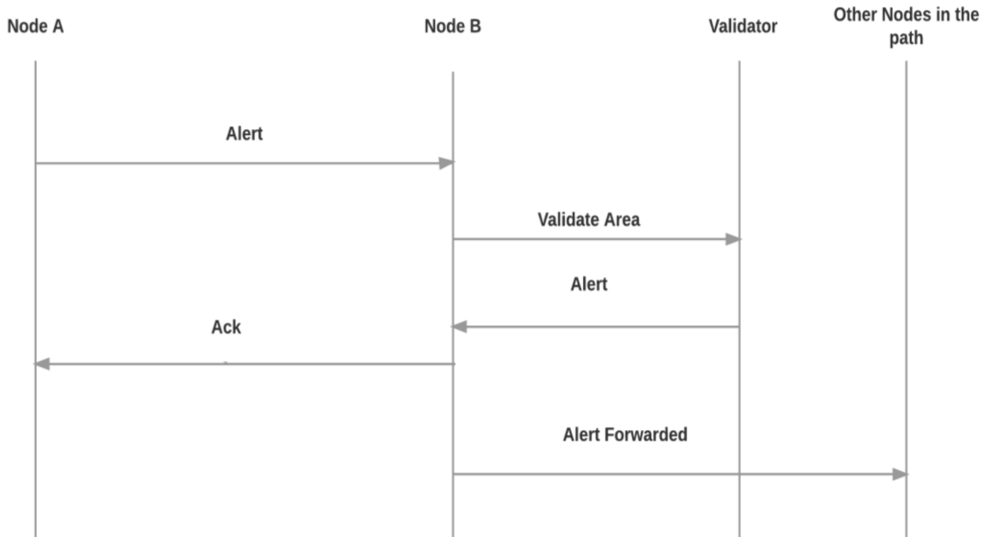

Fig. 8. Alert forwarding through the network.

5 Performance analysis

This section presents the energy consumption and probability of success measurements of our proposal. To test the performance of our mechanism, simulation is done through MATLAB. The model uses a network of trust as a protocol to send messages among sensor nodes in a WSN in order to detect or predict a fire.

5.1 Experiment description and total energy consumed

In order to take energy consumption measurements, we created five scenarios of our proposal and we simulated them so we could compare them. As we already described in previous sections, the WSN consists of sensor nodes and cameras. These cameras are responsible for verifying whether the alarm is true or not. If the alarm is true we consider the node that raised the alarm as trusted and, as a result, we raise the trust that its neighbours have in it. According to this, we can have a WSN with different number of trusted nodes. The five scenarios that we already mentioned are composed of a network with 100%, 80%, 60%, 40% and 20% of trusted nodes. The simulated systems disable every node that sends a false positive. Those systems disable that node for the entire simulation. Besides, nodes do not compute the different levels of trust. In our experiments, the first false positive causes a node disabling.

Fig. 9 shows the total relative energy consumption of our proposal. As we can see from the graph, from 20% to a 100% of trusted nodes there is an exponential growth of the energy consumption, starting from 15% and reaching a 100% of energy consumption that corresponds to the total energy consumed with the 100% of the nodes connected. The rest of this section extensively analyzes the individual energy consumption of each scenario and the probability of success.

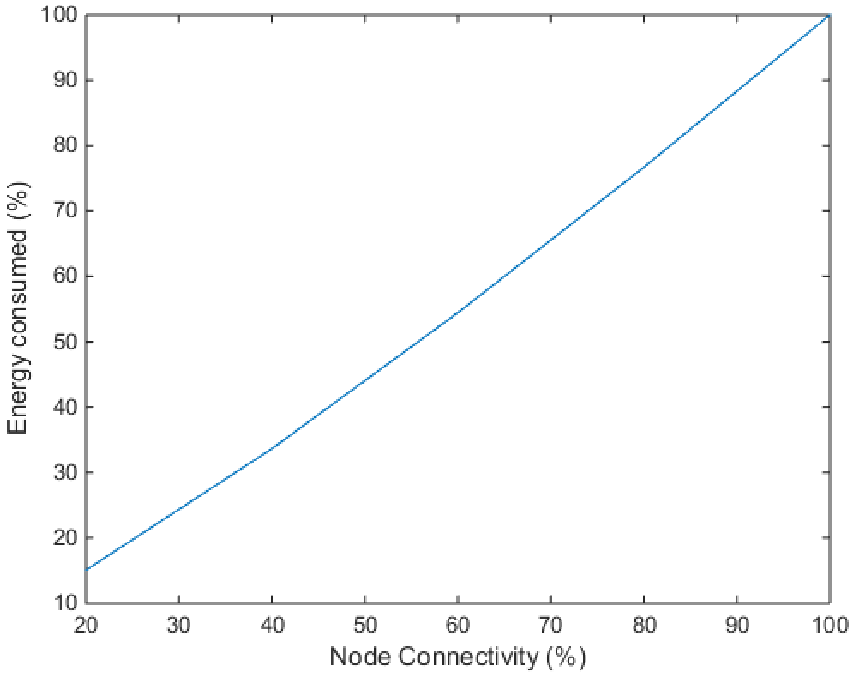

Fig. 9. Total relative energy consumption attending to the connectivity on the network.

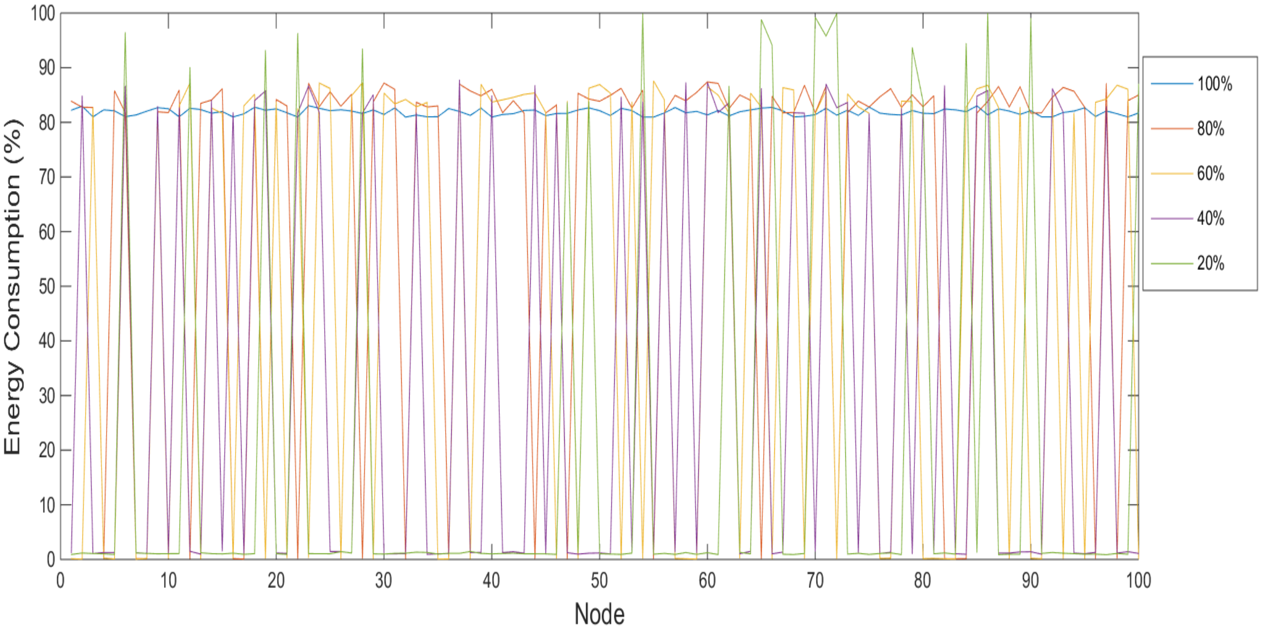

Fig. 10. Relative energy consumed by each node in all the scenarios.

5.2 100% Node Connectivity

In the first scenario, we consider an ideal network, where all of the nodes are trusted. Fig. 10 shows the energy consumption of each node in all five scenarios. The energy consumption is relative, being the 100% value the higher energy consumed by a node in all the scenarios. There are five different color lines, one for each case. In particular, the first scenario is being described by the blue line. As can be seen at the graph, we have the biggest average of energy consumption (approximately 83%). The graph is like a straight line without any considerable fluctuations. The upper limit is a 84% of the energy consumption and the lowest limit is a 82% of total energy consumption.

5.3 80% Node Connectivity

In this scenario, there is trust on 80% of the nodes, the rest 20% are nodes that produced false positives and they are dismissed from the trusted network for the entire simulation. They can be either malicious or just had a bad prediction. This case is presented in Fig. 10 as the orange line. As we may notice from the graph, this scenario is close to the previous one but with some significant differences. The peak of the energy consumption is 87%, but the minimum is near 0%. This happens because not all nodes of the network are trusted so they only take part in the network of trust for a period of time. As a result, the graph of this scenario has sharp fluctuations but we can notice that the time where the level of energy consumption of every node is around 85% is bigger than the time where every node has close to 0% energy consumption.

5.4 60% Node Connectivity

Subsequently, we present a scenario where 60% of the nodes take part in the trusted network. Yellow line of Fig. 10 shows the tendency of this scenario. The results of this scenario are close to the previous one. Energy consumption reaches 87% as a maximum rate and near 0% as minimum. The only substantial difference with the previous case is that the time when the energy consumption is in its peak is less. As a result, the average of the total energy consumption in this scenario is less than previous scenarios.

5.5 40% Node Connectivity

Purple line of Fig. 10 indicates the trends of energy consumption when 40% of the nodes in a WSN are not trusted. In this case, we may notice that there are abrupt fluctuations in the trend of the energy consumption in each node. No similarity with previous scenarios can be seen. There are only two options for every node, either it consumes energy equal to 84% or near 0%. No stability at the line can be noticed, this leads to low levels of total energy consumption. This is caused by the overload due to disabling nodes and recalculating the routing path to the gateway. Additionally, when an alert situation occurs in networks with low connectivity, more validations are required and more communications with the validators are done, which generates more traffic and more energy consumption.

5.6 20% Node Connectivity

Last scenario stands for a network where most of the nodes are not-trusted. Only 20% of them take place in the trusted network. Green line of Fig. 10 shows the results of this case. The graph is pretty much the same as the previous scenario. The only differences that can be noticed are that the energy consumption is most time near 0%. We can also see that the fluctuations are not as frequent as previous scenarios, but when we have an upward trend it can touch a 100% of energy consumption for a period of time, what means that it is the scenario where the maximum individual energy is consumed. This happens because sensor nodes communicate only with 20% of the nodes and this introduce an overload as explained in the previous subsection. This has, as a result, minimum total energy consumption as it can be seen in Fig. 9.

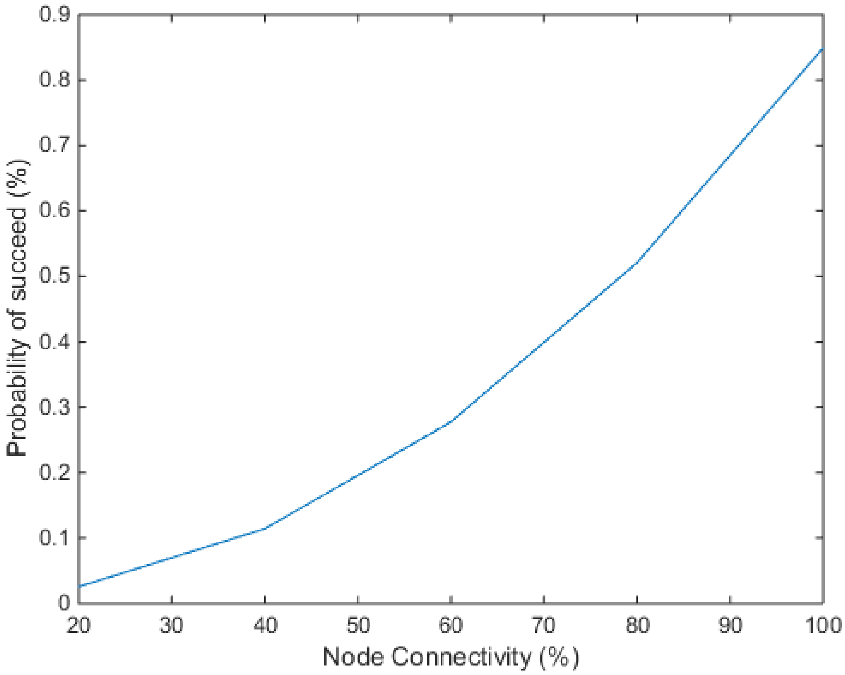

Fig. 11. Probability of succeed

5.7 Probability of succeed

On the other hand, it is very important to see the probability of success in case of a disaster (in our case fire). This measurement is the probability of having a fire, detect the fire and send the alarm report to the gateway across the network. In case of a true positive, a true alert, the probability of detecting the disaster and communicate with the gateway in order to report it is an important factor. As Fig. 11 indicates, the possibility of succeeding is between 3% and 85%, following an exponential trend depending on the amount of node connectivity. In the scenario when we have an ideal network where all sensors are trusted this probability reaches its peak rate. It is remarkable that when there is 80% node connectivity, the probability of success is approximately 50%. It is caused because some of the disabled nodes can be together in the simulation and provoke a connectivity loss.

6 Conclusions

In this paper, we have proposed a new false positive based model for establishing trust management between sensor nodes in a WSN, using camera nodes as validators, in order to reduce the energy consumption levels of each node and to eliminate the production of false positive alarms.

We have performed several tests to validate the benefits of our proposal. They showed us that not trusting all of the nodes in a WSN, can have better results in the total energy consumption of the network and in each sensor node individually. From the other hand, not having many participants in a WSN can reduce the probability of success and can also cause loss of connectivity of the entire network. Furthermore, with our simulated proposal, having a high number of malicious nodes increases the energy consumption on the rest of the nodes, due to the overload introduced by the disabling messages and by recalculating the routing path.

As a future work, many improvements can be done as well as more experiments or proposals. For instance, the importance of the validators can be tested and several proposals based on wondering the trust that nodes must have in them can be done. In addition, in order to save more energy, it is possible to design a routing protocol which takes into account the possibility of temporally disabling nodes.

References

Ministry of Agriculture, Alimentation and Environment of Spain (2016) Report on Forest Fires of 2015. Available at http://www.magrama.gob.es/es/desarrollo-rural/estadisticas/iiff_2015_def_tcm7-416547.pdf. Last accessed on October 30, 2016.

Akyildiz Ian F., Su W. and Sankarasubramaniam Y. (2002) “Wireless sensor networks: a survey”, Computer networks, vol. 38, no 4, p. 393-422. http://dx.doi.org/10.1016/S1389-1286(01)00302-4

Muhammad Adeel M., Winston K. G. S. and Welch I. (2015) “Reliability in wireless sensor networks: A survey and challenges ahead”, Computer Networks, vol. 79, p. 166-187. http://dx.doi.org/10.1016/j.comnet.2014.12.016

Dulman S., Nieberg T., Wu J. and Havinga P. (2003) “Trade-off between traffic overhead and reliability in multipath routing for wireless sensor networks”, Wireless Communications and Networking 2003, WCNC 2003, IEEE, p. 1918-1922. Http://dx.doi.org/10.1109/WCNC.2003.1200680

Lloret J., García M., Bri D. and Sendra S. (2009) “A wireless sensor network deployment for rural and forest fire detection and verification”, Sensors, vol. 9, no 11, p. 8722-8747. http://dx.doi.org/10.3390/s91108722

YU L., Wang N. and Meng X. (2005) “Real-time forest fire detection with wireless sensor networks”, Proceedings. 2005 International Conference on Wireless Communications, Networking and Mobile Computing, 2005. IEEE, p. 1214-1217. http://dx.doi.org/10.1109/WCNM.2005.1544272

Chauhan A., Semwal S. and Chawhan R. (2013) ” Artificial neural network-based forest fire detection system using wireless sensor network”, 2013 Annual IEEE India Conference (INDICON). IEEE, p. 1-6. http://dx.doi.org/ 10.1109/INDCON.2013.6725913

Liu Yo., Gu Y., Ji Y., and Li J. (2011) “A novel accurate forest fire detection system using wireless sensor networks”, Mobile Ad-hoc and Sensor Networks (MSN), 2011 Seventh International Conference on. IEEE, 2011. p. 52-59. http://dx.doi.org/ 10.1109/MSN.2011.8

Herutomo A., Abdurohman M., Anggis Suwastika N., Prabowo S. and Wirawan Wijiutomo C. (2015) “Forest fire detection system reliability test using wireless sensor network and OpenMTC communication platform”, Information and Communication Technology (ICoICT), 2015 3rd International Conference on. IEEE, p. 87-91. http://dx.doi.org/ 10.1109/ICoICT.2015.7231402

Al-Abbasss Y. A. and Ahmed M. H.; HUSAIN (2011) “Taher. Reliability analysis of Wireless Sensor Networks for forest fire detection”, 2011 7th International Wireless Communications and Mobile Computing Conference. IEEE, p. 1630-1635. http://dx.doi.org/ 10.1109/IWCMC.2011.5982779

Srinivasan A., Teitelbaum J. and Wu J., (2006) “DRBTS: distributed reputation-based beacon trust system” 2006 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing. IEEE, p. 277-283. http://dx.doi.org/ 10.1109/DASC.2006.28

Bonatti P., Duma C., Olmedilla D. and Shahmehri N. (2007) “An integration of reputation-based and policy-based trust management”. *networks*, 2007, vol. 2, no 14, p. 10.

Li X., Zhou F. and Du J. (2013) “LDTS: a lightweight and dependable trust system for clustered wireless sensor networks”, IEEE transactions on information forensics and security, vol. 8, no 6, p. 924-935. http://dx.doi.org/ 10.1109/TIFS.2013.2240299

Shaikh R., Jameel H., d’Auriol B., Lee H., Lee S. and Song Y. (2009) “Group-based trust management scheme for clustered wireless sensor networks”. IEEE transactions on parallel and distributed systems, 2009, vol. 20, no 11, p. 1698-1712. http://dx.doi.org/ 10.1109/TPDS.2008.258

Shaikh R., Jameel H., Lee S., Rajput S. and Song Y. (2006) “Trust management problem in distributed wireless sensor networks”. *12th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA'06)*. IEEE, 2006. p. 411-414. http://dx.doi.org/ 10.1109/RTCSA.2006.61

Bao F., Chen I., Chang M. and Cho J. (2012) “Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection”, IEEE transactions on network and service management, 2012, vol. 9, no 2, p. 169-183. http://dx.doi.org/ 10.1109/TCOMM.2012.031912.110179

Ninghui L., Mitchell J., Winsborough W. (2002) “Design of a role-based trust-management framework”, Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on. IEEE, 2002. p. 114-130. http://dx.doi.org/ 10.1109/SECPRI.2002.1004366

Han G., Jiang J., Shu L., Niu J. and Chao H. (2014) “Management and applications of trust in Wireless Sensor Networks: A survey”, Journal of Computer and System Sciences, 2014, vol. 80, no 3, p. 602-617. http://dx.doi.org/10.1016/j.jcss.2013.06.014

Zahariadis T., Leligou H., Trakadas P. and Voliotis S. (2010) “Trust management in wireless sensor networks”, European Transactions on Telecommunications, 2010, vol. 21, no 4, p. 386-395. http://dx.doi.org/ 10.1002/ett.1413

Lopez J., Roman R., Agudo I., and Fernandez-Gago C. (2010) “Trust management systems for wireless sensor networks: Best practices”, Computer Communications, 2010, vol. 33, no 9, p. 1086-1093. http://dx.doi.org/10.1016/j.comcom.2010.02.006

Weeks S. (2001) “Understanding trust management systems”, Security and Privacy, 2001. S&P 2001. Proceedings. 2001 IEEE Symposium on. IEEE, 2001. p. 94-105. http://dx.doi.org/ 10.1109/SECPRI.2001.924290