BYZANTINE DECISIONS FOR INFERRING TRUST IN SENSOR NETWORKS

Björn Stelte
Institut für Technische Informatik, Universität der Bundeswehr München, Munich, Germany

Keywords: Byzantine decision, Wireless sensor networks, Gaussian trust and reputation system, Trust.

Abstract: A secure Wireless Sensor Network consists of highly secured and trustworthy sensor nodes. But making one single node secure is impossible due to low computational power, memory and cost constraints. Sensor nodes are not tamper proof nor will be in future. In our concept we use low-cost redundant sensors and the Byzantine Fault Tolerance to overcome attacks on the network especially concerning insider attacks. Every sensor node calculates a trust-level of its peer neighbors by a Bayesian probabilistic reputation system. An efficient real-time based communication protocol is used to reduce communication overhead and to transport local trust-levels to the gateway node to calculate a common trust-level.

1 INTRODUCTION

We need trustworthy wireless senor networks (WSN) in the future otherwise information delivered by sensor networks will be useless for the operator and in particular for urgent decision making. Dependent on the used scenario malicious behaving nodes or attacks on the WSN will be more or less harmful. Regarding scenarios where critical infrastructure is monitored or even in military scenarios, a highly trustworthy WSN is needed to monitor events and report data. Sensed data represent the core component of trust-modeling in a WSN. A trust-based system has to discover and exclude misbehaving nodes as well as minimizing the risk of inside attacks.

As addressed by e.g. ISO-10181 and ISO-27001 confidentiality, integrity, availability, etc. are to be regarded to deploy trustfully and secure WSNs. Sensor networks somehow share the same vulnerabilities as those in any open network offering end-to-end connectivity. Also specific vulnerabilities arise due to the fact that sensor nodes depend on a non-changeable battery, such as sleep-deprivation attacks where the attacker generates spurious activity so that nodes, will waste their battery power within a short period.

A trustworthy WSN needs beside secure communication trustworthy components, so each sensor node should be implemented as much secure as possible. Several concepts exists but these concepts will only work under the assumption that it is possible to build cheap and powerful tamper proof sensor nodes. In the following, we suppose that every sensor node is vulnerable regardless of the used security system.

Different research communities have defined the term trust differently. In this paper we define trust as "THE SUBJECTIVE PROBABILITY BY WHICH NODE A DEPENDS ON NODE B TO FULFILL ITS PROMISES IN PERFORMING AN ACTION AND AT THE SAME TIME BEING RELIABLE IN REPORTING ITS SENSED DATA" (Momani and Challa, 2007).

Trust-modeling can be defined as the mathematical representation of a node's opinion of other nodes in the network. The trust-modeling problem is a decision problem concerning which nodes are to be trusted.

Momani has introduced a Bayesian probabilistic reputation system and trust model called Gaussian Trust and Reputation System for Sensors Networks (GTRSSN) (Momani and Challa, 2007). This Bayesian probabilistic approach for modeling trust in WSNs in the case of continuous sensor data can be extended. So far this approach only estimates the trust between two connected nodes (peer) and every node stores the calculated trust-level of its peer neighbors. Therefore, we see the need for two extensions of the approach: sharing the trust-level with other peer nodes to calculate a common trust-level concerning the node and the a real-time based communication.

The following section introduces the GTRSSN approach on which our concept is based. Section 3 introduced the idea how to efficiently store and communicate trust-level values efficiently with a real-

Stelte B..
BYZANTINE DECISIONS FOR INFERRING TRUST IN SENSOR NETWORKS.
DOI: 10.5220/0003524903960399
In *Proceedings of the International Conference on Security and Cryptography* (SECRYPT-2011), pages 396-399
ISBN: 978-989-8425-71-3

time, blackboard-based publish/subscribe system for WSNs. In Section 4 we will show our concept of an Byzantine agreement approach to find a common decision concerning the common node-trust problem based on the three concepts GTRSSN, Byzantine decision making, and real-time communication. Finally Section 5 concludes our work.

2 GAUSSIAN TRUST AND REPUTATION SYSTEM

As defined by Momani modeling trust in general is the process of representing the trustworthiness of one node in the opinion of another node. The two main sources for trust formation are the direct observation of the behavior of neighbor nodes and the recommendation from other nodes (Momani and Challa, 2007). The indirect trust represented by the recommendation is also called second-hand information. Figure 1 shows the general trust computation model.

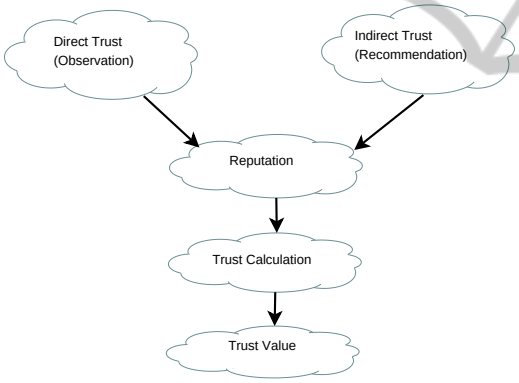

Figure 1: Trust Computational Model.

The idea behind the GTRSSN approach is that a sensor node will observe neighboring nodes' behavior and calculate a reputation for that node based on the observed data. The procedure behind GTRSSN can be explained by a short example. In a given sensor network all surrounding nodes connected to a sending node hear the reported value (1-hop distance) and interpret this as a direct observation. Each node now calculates its trust value between them and the sending node. Therefore the own sensed value and the reported value are used. This new calculated value is later send to the recipient node as a second-hand information. The recipient node can recalculate the trust between him and the sending node based on direct (observation) and indirect (recommendation) trust values.

The GTRSSN trust model defines trust to be the probability (*Prob*) as shown in the following equation:

$$\begin{aligned} T_{i,j} &= Prob\{-\varepsilon < \theta_{i,j} < +\varepsilon\} \\ &= \phi\left(\frac{\varepsilon - \mu_{i,j}}{\sigma}\right) - \phi\left(\frac{\varepsilon - \mu_{i,j}}{\sigma}\right) \end{aligned} \tag{1}$$

where $\theta_{i,j}$ is the calculated error, ϕ is the cumulative probability distribution of the Normal $N(0,1)$, $\mu_{i,j}$ and ${\sigma^2}_{i,j}$ represent the mean and variance. Or in other words, the trust value is the area under the Gaussian curve $N(\mu_{i,j}, {\sigma^2}_{i,j})$ within the interval $[-\varepsilon, +\varepsilon]$ as shown in Figure 2.

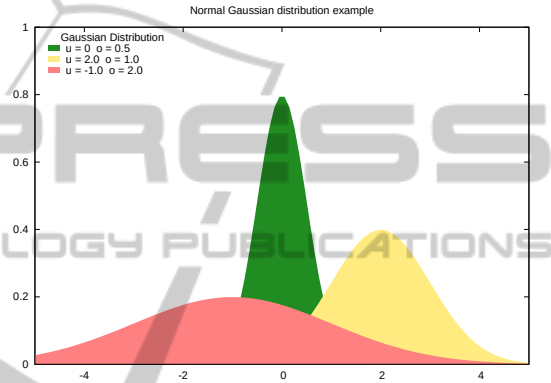

Figure 2: Normal Gaussian distribution example.

The smaller the error $\theta_{i,j}$ is the higher will the trust be. The more spread the error is, and its mean shifting to the left and right of 0, the lower will the trust value be. The trust value $T_{i,j}$ is updated for each time period a message is received from node j. The second hand information is used to recalculate $\mu_{i,j}$ and ${\sigma^2}_{i,j}$.

The problem is that the GTRSSN approach is not enough. Malicious nodes (being captured by an enemy) could easily drop information or spread malicious data. As only the recipient of a message gets a second hand information provided by other nodes in its surrendering, it is necessary that at least one node calculates a trust connection value under a certain threshold so that common decision making can be established to determine the trust of the node. In the next section we will briefly describe a message transport approach to distribute trust values.

3 EFFICIENT MESSAGE TRANSPORT UNDER REAL-TIME CONSTRAINTS

In a distributed system like a WSN it is advantageous to decouple the communicating components from

each other regarding time, space, and synchronization (Eugster et al., 2003). With these communication decoupling nodes of a WSN operate as autonomously as possible. It suggests that a system following the publish/subscribe paradigm fits the nature of WSN communications. A publish/subscribed based event message management system for WSNs has to show that it is possible to have a publish/subscribe paradigm based message system in WSN on the one hand but also to combine real-time functionality to a WSN message system on the other hand. So far, as we know, only few research results are published concerning real-time publish/subscribe in WSNs, while publish/subscribe itself next to real-time, and data distribution for WSN is discussed widely

In a WSN, sensor nodes placed randomly in the environment detect events like for e.g. a sharp rise of temperature. Actor nodes in the network react on an alert message by for e.g. closing a valve or activating an alarm. Gateway nodes distribute messages send by sensor nodes to monitor equipment placed outside the WSN. Communication overhead in such a scenario will reduce the total run-time of the WSN as power consumption is the mean problem. In the outlined publish/subscribe driven concept actors (maybe also the gateway as required) tell the sensor nodes that they are interested in a certain event and that the message should be delivered in a certain time. So the actor nodes transmit a subscription to sensor nodes, whom notify the subscribers (actor nodes) within the given time period if an event is detected and the event fulfills the subscription.

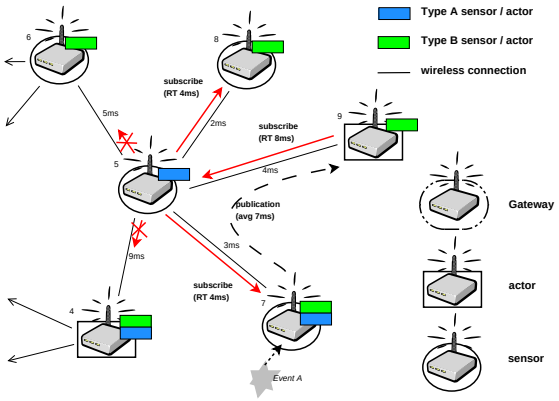

Figure 3: Example of efficient message communication.

Figure 3 shows a typical scenario of a WSN with 4 sensor nodes and 2 actor nodes. In the start phase ACTOR NODE 9 (right side) sends a subscribe request message to all reachable nodes. In this scenario only SENSOR NODE 5 is reachable that receives the request. As SENSOR NODE 5 only monitors events of type A and ACTOR NODE 9 requests to get informed about type B events the sensor node only proves that the deliverable time is lower than the requested maximum deliverable time. In this case the deliverable time is in average 4 ms and the subscriber needs a notification within 8 ms. Therefore, SENSOR NODE 5 will forward the subscription request to all its neighbors, here nodes 8, 6, 4, AND 7. NODE 4 is an actor node and will neglect the request, next to SENSOR NODE 6 which can calculate that the real-time constraint can never be fulfilled as the deliverable time on the route back to the requester will take too long. Only SENSOR NODE 8 and 7 can notify the requesting node in-time. Both sensor nodes monitor events of Type A which fulfills the received subscription request and will store the subscription locally. Since the remaining deliverable time is very low and calculation and notification packet calculation have to be considered, the sensor nodes will not try to forward the request to other neighbors. The presented concept for efficient message transportation by a real-time enabled publish/subscribe system can be used to distribute trust values. Therefore, the calculated trust value represents a parameter for a subscription rule. If this rule is fulfilled all subscribed nodes with one-hop distance will get informed. The publish/subscribe system is flexible in such that if a connection to a node is disturbed a subscription could be deleted or if a new connection is established a new subscription could be registered. For further details have a look at (Stelte, 2011).

Next we will show that it is possible to use the Byzantine decision algorithm to find a common majority decision based on reported trust values.

4 BYZANTINE DECISION

The name Byzantine Attack is based on the Byzantine Generals' Problem which is a generalized version of the famous Two Armies Problem.The Byzantine Generals' Problem was first introduced by Lamport et al. in (Lamport et al., 1982). It describes a decision problem where one Commander in Chief and $n-1$ generals communicate with each other. The communication between two persons is handled over a synchronous and non error-prone communication channel. The commander informs his generals the decision to attack or to retreat. The action is successful only if all generals carry out the instruction of the commander. In this scenario it is possible that at least one person (general or commander) tries to tamper. Goal of a Byzantine protocol is to let the honest generals come to a collective decision (under the as-

sumption that the commander is honest). Lamport et al. have formulated the thesis that for n persons with k betrayers there is a communication protocol that leads to a common decision if and only if $n \geq 3k+1$. In (Lamport et al., 1982) the proof of this thesis can be found.

With the GTRSSN reputation system every node will calculate a trust value concerning its connection to neighbor nodes. This only locally used trust value helps other nodes in the network and especially the gateway node of the network to decide if a communication to a certain node should be neglected or not. Therefore, calculated trust values should be delivered to the gateway node if at least one trust value is under a certain threshold. An efficient middle-ware is needed to do the job. As mentioned before we use in our concept a real-time based publish/subscribe system to spread the information. To avoid an action of the supposed untrusted node all connections to these node (routing table) will not be used. So other nodes in the network have to forward the information to the gateway node. Figure 4 shows this procedure, where Node 2 sends an event message to the gateway node. After all neighbor nodes have calculated their own trust value $T_{i,2}$ they report to the gateway node if they are in a one-hop distance (here only Node 4). If we assume that, for e.g. Node 3 calculates a bad trust value (the node is near but monitors completely different values), Node 3 will inform its neighbor nodes about a trust voting concerning Node 2. Node 2 can not anymore being used as router node, so Node 6 has to be used by Node 3. After some rounds every node has reported its value to the gateway node (path 3-6-5-4-1). The gateway node can now fill a trust table with all received trust values. The values in this trust table for Node 2 can be used in a Byzantine decision making process to find a majority decision if Node 2 and its values are trustworthy or not. Therefore, all continuously GTRSSN trust values have to be mapped to a binary value T_node, where the value is 1 if the trust value is below 0.5 and set to 0 otherwise. We have implemented our architecture on sensor nodes and we have experienced that an additional aging factor is necessary to reduce trust value fluctuations. The right choice of this aging factor is a tradeoff between response time and false-error rate. We will further investigate how to choice the factor in awareness on the operational environment smartly.

In this concept the gateway node is the trustworthy connection point. Only a gateway node needs a tamper proof hardware which reduces the costs significantly. The assurance level depends on the amount of active sensor nodes and is variable concerning the users requirements. Also, power consumption for the

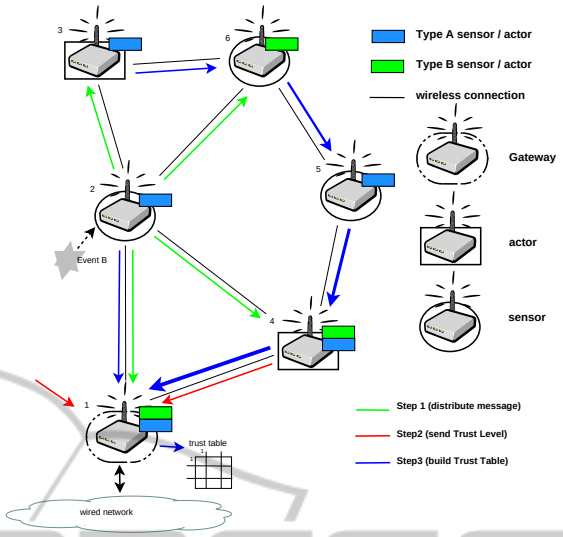

Figure 4: Example of Bayesian estimation of trust with Byzantine decision making.

voter is not an issue. Depending on the amount of corresponding nodes and their reported values the gateway node can decide if reported values from Node 2 should be forwarded or all nodes in the network should be informed about a misbehaving node.

5 CONCLUSIONS

The introduced concept combines the GTRSSN reputation system, an efficient message transport approach, and the Byzantine agreement concept. This concept is realizable under the specific sensor network requirements and enriches trust in such networks. Therefore, the presented idea is of high interest especially if sensor networks are used for urgent decision making such in military and disaster control scenarios.

REFERENCES

Eugster, P. T., Felber, P. A., Guerraoui, R., and Kermarrec, A.-M. (2003). The many faces of publish/subscribe. *ACM Comput. Surv.*, 35:114–131.

Lamport, L., Shostak, R., and Pease, M. (1982). The Byzantine Generals Problem. *ACM Trans. Program. Lang. Syst.*, 4:382–401.

Momani, M. and Challa, S. (2007). GTRSSN: Gaussian Trust and Reputation System for Sensor Networks. In *SCSS (1)*, pages 343–347.

Stelte, B. (2011). An Event Management System for Wireless Sensor Networks. In *IEEE IM 2011 - TechSessions*, Dublin, Ireland.