Secure Reputation Update for Target Localization in Wireless Sensor Networks

Tanuja R.[1], Anoosha V.[1], Manjula S.H.[1],
Venugopal K.R.[1], Iyengar S.S.[2], and L.M. Patnaik[3]

[1] Department of Computer Science and Engineering,
University Visvesvaraya College of Engineering, Bangalore University, Bangalore
r_tanuja@yahoo.com
[2] Florida International University, USA
[3] Indian Institute of Science, Bangalore

Abstract. Wireless Sensor Networks (WSNs) are by its nature more prone to security attacks and data losses. Security and data privacy have become need of the day. The most challenging area in WSNs which needs security is target localization. In addition to this complexity we are here concentrating on acoustic sensor nodes which uses Particle Swarm Optimization (PSO) algorithm for Location Estimation. We propose Secure Reputation Update Target Localization (SRUTL) algorithm which addresses target localization and security issues viz., bad-mouth attack, Sybil attack, on-off attack and malicious node attack at different levels of target localization. Simulation results shows positive response in attack detection hence contribute in building a secure wireless sensor network.

Keywords: Insider Attacks, Security, Reputation System, Target Localization, Wireless Sensor Networks (WSNs).

1 Introduction

Wireless Sensor Networks are known for their environment sensitive data collection and analysis which helps to solve most of the real world problems. Besides its resource constraint characteristics like, limited battery power, bandwidth, limited memory and network characteristics like, unreliable communication, higher latency, etc., it has emerged as a platform for signal processing and communication. Geographical information is one of the most important parameter in WSNs. The data stream is relevant only if location information of monitoring event is known. This issue is usually known as acoustic target localization (ATL) problem. Along with sensing, computing and communicating, the WSNs should also provide security to the sensor network.

Military base, which requires fast and accurate location information of its groups and secure channel to guard against enemy intervening our military signals can explain why ATL problem is so important in WSNs. In this scenario, the communication network should be fast and accurate with less overhead and

K.R. Venugopal and L.M. Patnaik (Eds.): ICIP 2012, CCIS 292, pp. 109–118, 2012.

at the same time defend itself against various attacks like node compromise, replay attack, malicious nodes, etc., from the other side. Another example to show importance of ATL problem is vehicle monitoring scenario. As sound emitted by vehicles are not Omni-directional, target location estimation become complex. The complexity increase with addition of environmental noise, multi targets presence and thus the robust reputation system come to the rescue.

The target location estimation in WSNs can be performed using either centralized or de-centralized localization techniques. Reputation system provides a method of de-centralized localization, wherein every node is qualified based in its reputation score to perform target estimation. This helps in achieving node level security issues viz., false node (may be faulty node), node malfunction, node outage and physical attacks in WSNs. The resources and information communicated in WSNs should be protected and as well as defend security attacks. Most important security measures that should be addressed are : Data Confidentiality, Data Integrity, Availability, Data freshness, Self-Organization, Secure Localization, Time Synchronization and Authentication.

Secure Localization, determines accuracy and automatic location estimation in WSNs. Defending attacks on target localization networks which can be using either range-based or range free techniques, is a potential problem. Our proposed scheme addresses this issue. Reputation is vital to achieve security in a non-cryptographic scenario. This helps in analyzing untrustworthy sensors which hamper the network performance. By data synthesis (fusion) process on each nodes reputation score helps in reducing impact of faulty or malicious nodes in WSNs. Reputation computation is a challenging task as it should be strong enough to sustain internal attacks in WSNs. Previously, a watch-dog module was used to monitor nodes behavior, but this is a high energy consumption technique. Thus to ensure lower energy usage and better network functioning, a reputation system here is built based on powerful *Dirichlet distribution*.

Motivation: Researches have derived several algorithms and techniques which provide location estimation, high performance factor, low communication cost, defense against various attacks like wormhole attack, Sybil attack, node malfunction etc., but with their own drawbacks. None of them combine the efficiency and security for target localization in WSNs, which is our area of interest. With the help of better security framework which can overcome some of the most dangerous attacks in WSNs along with a highly efficient target localization scheme to address the current challenge in WSNs.

Contributions: We propose a new algorithm known as Secure Reputation Update for Target Localization (SRUTL). This scheme adds security measures to the existing reputation system in acoustic WSNs. The main focus is on secure update of reputation value at each individual node during transmission control phase. A node is allowed to increase its reputation if and only if its sensed data has contributed in location estimation. If there is a sudden increase or decrease in reputation value, then that node is ignored from the network. When a faulty node enters back to network, it will be given initial reputation score as assigned

during deployment phase, thus protecting the whole network from malicious nodes and safeguarding network performance.

Organization: The rest of the paper is organized as follows: Section 2 deals with study of previous techniques in support to the proposed system. Section 3 gives background work and base algorithms used in our system. The acoustic sensing model and proposed SRUTL algorithm are explained in Section 4. Section 5 gives implementation and performance evaluation. Section 6 gives conclusions and future enhancement.

2 Related Works

Many applications find WSNs advantageous than compared to other networks. A data without its origin is insignificant. Thus a sensed data signal in any WSNs is only valid until its source location is known, which is commonly addressed as Acoustic Target Localization (ATL) problem in WSNs. A simple scenario to explain ATL problem is shown in the form of localization in [1] using two step Acoustic mapping for multiple speakers based localization. It shows a comparative study of Global Coherence Field (GCF) and Oriented Global Coherence Field (OGCF) techniques which are widely used.

Zaher et al.,[2] have proposed a EB-MAC protocol for event-based system that characterizes acoustic target location system using Time Difference on Arrival (TDOA). Fuzzy Art data fusion center is designed to detect errors and fuses estimates to a decision based on spatial correlation and consensus vote. On MICAZ motes with Tiny-OS this protocol provides reliable fault tolerant communication platform that maximizes throughput, lowers channel contention and latency with huge enhancement over other fusion algorithm. It has a drawback of single point failure and performance poorly in dense sensor networks and outdoor deployments.

Alexander et al.,[3] have demonstrated an automatic self-localization scheme using non parametric belief propagation (NBP) for location estimation and resending uncertain location information. As its implemented in distributed environment it helps various statistical models and multi-model uncertainty. It has low cost in-terms of messages per sensors and low bit rate approximation for messages which results in no impact on network performance. This method is extensible to non-Gaussian noise models so as to increase robustness of the network. Other message-passing inference algorithm viz., max-product might help to improve performance which is not considered here. Also alternative graphical models can provide more accuracy than that of the proposed NBP technique. NBP can serve as a useful tool for estimating unknown sensors location in large ad-hoc networks.

Pramod et al.,[4] have described a new approach for target localization which uses quantized sensor data and channel statistics of WSNs. This novel approach uses Cramer-Rao Lower Bounds (CRLBs) for location estimation. Three different types of target location estimators are developed for various link layer designs viz., Hard decoding Binary-Channel (BC), Soft decoding in Rayleigh

Fading Channel with Coherent Reception and Soft decoding in Rayleigh Fading Channel with Non-coherent Reception. A channel-aware estimator is derived from CRLBs even with a relatively small number of sensors. Results show coherent reception scheme performance better that non-coherent reception scheme for both soft and hard decoding links. Improve localization performance by designing an optimal local sensor threshold needs to be addressed. This scheme can be incorporated in larger dimensions of performance optimization by adding physical layer parameters and other functional characteristics such as various modulation and coding schemes. This can be generalized to extend for multiple target estimation scenarios.

Most of research works on ATL problem either design localization algorithms [5] or target estimation schemes [6] for a better solution in WSNs. These localization algorithms are required to report the origin of event, assist group querying of sensors, routing and answering questions on the network coverage. Whereas target estimation schemes concentrate on specific parameters like, using mobile agents for collaboration and classification, mobile anchor nodes [7], channel aware data quantization to find location information.

One of the most efficient algorithm for target localization is known as Particle Swarm Optimization (PSO) which is described in Raghavendra et al., [7], Xu et al., [8], Panigrahi et al., [9], along with Xue et al., [10] which is base of this paper. All the above works have explored PSO in different direction like network-centric, mobile anchor assisted, maximum likelihood function etc., to arrive to one simple solution for ATL problem. Most of their experiments were carried out using MICAz motes. The acoustic network model is derived from [10], which help in providing a realistic network view.

3 Background

Reputation system designed for accurate target sensing in WSNs, provides security at each individual node[10]. Based on weighted measurement of each node in data fusion a reputation is calculated and thus effect of untrustworthy nodes is eliminated from the network.(i) All the initial network parameters assigned while building sensor network model and acoustic sensing model. (ii) Each nodes rating value is expressed by its probability distribution of measurement error (PDME) of possible outcomes along with positive real parameters which is efficiently expressed using Dirichlet distribution for variable vector and parameter vector. (iii) Reconstruction of the sensing model is carried out with pre-defined threshold for along with its rating bounds, to detect a targets existence. By solving an objective function of least-square estimation as in [2] helps to determine sensing parameters along with deviation factor from true measurement.

The earlier works concentrates only on target location estimation with high accuracy, reliable data delivery and node failure due to physical tampering and high inter-device or environmental noise. Our concern is to make a realistic secure model for ATL which can protect itself from most common WSN attacks like bad-mouth attack, Sybil attack, on-off attack and malicious nodes.

Table 1. Notations used in the Algorithm

Symbols	*Definition*
S_{ssth}	sensed signal strength threshold
s_i	sensed data at node i
g	sensor gain
c	sensor measurement bias
NS_R	neighbor set reputation value
NS_{status}	neighbor set node status
r_i	reliability of node i
r_{ij}	link reliability between node i and j
γ	stability value
R_{th}	threshold value of reputation
R_i	reputation value of node i

4 Problem Definition and Algorithm

4.1 Problem Definition

Given a set of Wireless Sensor Nodes $S_i \in V$ where $i = 1, 2, \ldots, n$ as an acoustic sensor network established by either throwing sensor nodes through an air bound vehicle to the fields where the data has to be read from stationary objects and target object is expected to pass by through the designated region. These sensor nodes have to sense data and provide location estimation. There may be a faulty node or malicious node estimation which should be identified and discarded.

The objectives of the algorithm are :

(i) Calulate reputation trust values and estimate target location.
(ii) To make a realistic secure model which can protect itself from most common WSN attacks like bad-mouth attack, Sybil attack, on-off attack and malicious nodes.

4.2 Algorithm

The proposed scheme provides a security framework for WSNs used for target location estimation. We introduce new algorithm, Secure Reputation Update for Target Localization (SRUTL) to securely modify reputation value at each node.

There are three phases of the algorithm applied at three different levels.

Phase1. After construction sensing model for the uniform distributed WSNs using Dirichlet distribution and least square estimation, stability factor every node is verified. This can be same as trust value (or inter-device noise) of that node. This prevents malicious attack and on-off attack at node level. Later these nodes are considered as Cluster Members (CMs).

Table 2. Secure Reputation Update for Target Localization (SRUTL)

Phase 1: Create cluster members

begin
Initially γ is set to 0.5 and all nodes are considered normal.
for every node i
if event sensed AND $s_i \leq S_{ssth}$ then
broadcast ID Packets consisting of position and bias.
update γ by 0.1 and nodes status as Cluster Member(CM). **else**
wait for an event.
endif
endfor
end

Phase 2: Create cluster decoders

begin
for every node i $\in$ set of CMs
if $w_i \leq 500$ then
apply local voting algorithm to neighbor set NS of node i
for every node j, $R_j \leq R_{th}/2$ | j $\in$NS$_R$AND NS$status$
update γ by 0.15 and nodes status as Cluster Decoder(CD).
calculate r_j and r_{ij}
endfor
else
apply local voting algorithm to neighbor set NS of node i
along with prior value.
for every node j, $\gamma_{\ j} \geq 0.7$ AND $R_j \leq R_{th}$
update γ by 0.15 and nodes status as Cluster Decoder(CD).
update r_j and r_{ij}
endfor
endif
endfor
end

Phase2. After applying local voting scheme [10] for data filtering, the nodes identity is verified. This helps in detecting malicious nodes and defends against Sybil and on-off attacks, in turn efficiently identify Cluster Decoders (CDs.)

Phase3. During the process of execution of PSO algorithm at Cluster Heads (CHs), if a CH disconnects with the network then second highest reputed and stable CD is promoted as CH and carries its task. The probability of second elected CH suffering on-off attack is very less and thus can guarantee smooth network performance.

Table 2 shows the first two phases of the algorithm. During the first phase the nodes may be experience malicious attack and onoff attack. The nodes with faulty data (stale data) could be identified based on carefully selected signal strength threshold. So to next phase the nodes which are verified to be normal are added to cluster member set. The stability value assigned to each node plays a major role in selecting nodes which can resist it from the security attacks that

Table 3. Secure Reputation Update for Target Localization (SRUTL)

Phase 3: Create cluster Heads

begin
while ($num_{ch} \leq 2$)
for every node $_i \in$ set of CDs
exchange new trust value with other CDs
if $\gamma_{\ i} \leq 0.7$ OR 0.8 AND $R_j \leq R_j \mid$ j $\in$ set of CDs-node i **then**
elect that node as Cluster Head(CH) ; num_{ch}++
endif
endfor
endwhile
// Applying PSO algorithm
for every node $_i \in$ set of CHs
apply PSO algorithm.
calculate approx. $S_j \mid$ j $\in$ set of CDs and inform all other CDs.
verify the newly calculated S_j with precalculated approx. S_j
if no match **then**
broadcast node j is malicious node and update its status as faulty.
decrement R_j and γ_j
else
update its status normal and increment R_j and γ_j
endif
endfor
end

are interested. It also accounts the accumulated evidence matrix to determine nodes behavior. The difference in position information exchanged in ID packet to the one known at deployment phase should not exceed error_threshold [10].

In phase two, initially when communication has not crossed window size w=500, the local voting algorithm is applied on neighboring set of CMs. Then the nodes with higher rating level and valid status information, updates stability value and consider it as CDs. Meanwhile, nodes reliability and link reliability is also calculated. If the prior communication history is available then it contributes in estimating nodes behavior and thus reduces number of faulty nodes.

Table 3 shows the phase 3 of the algorithm. The following steps take place during phase 3 at CHs : (i) If the node is a cluster head then, estimate target location and then send update packet which contains, new target location and that nodes contribution factor using nodes sensed data reading, s_i. Else, wait for the cluster heads response for the nodes measurement epochs. (ii) Once update packet is received (which is unique), the nodes compute reputation based on its contribution for the target estimation by computing its new $s_{i,new}$ and increase its score accordingly using : $s_i = g_i a_i + n_i$, where a_i is the signal strength at every sensor node which is a polynomial distance function, n_i is combination of sensor network parameters like environmental and inter device noise which can determine nodes status. The cluster heads will increase its score once it sends

out update packet to its members. (iii) During next ID packet communication it includes its position, sensed data along with its new reputation score R_i, which will be verified by its cluster head of previous iteration. (iv) If a mismatch is found, that node is ignored for any further computation in the network. If it retunes back as normal node then its given initial reputation score and allowed to participate in location estimation, but will be taken into account only after crossing pre-determined threshold reputation score R_th, which is monitored consistently.

Every node in the network stores the reputation value of its neighboring node set along with its status (active/ inactive) information. By applying the above algorithm a reputation score is checked to identify any abnormal nodes behavior. Reputation score updation is applied and monitored by current CHs. While selecting a node as Effective Node the participating Featuring Nodes should verify that it is not an abnormal/ malicious node. The communication from the estimated target information of Effective Node to sink should be decided based on nodes and links reliability factor (50% of each). Once a node is identified as malicious by a rapid increase in its reputation score, should be ignored by the network.

5 Implementation and Performance Evaluation

5.1 Simulation Setup

We evaluate the performance of our scheme by simulation conducted in MATLAB with a 100x100 units region under observation. The nodes are uniformly distributed and targets are assumed to be randomly placed. All the network parameters are initialized at deployment phase and all nodes are assumed to be normal. This algorithm is distributed in nature and stability is achieved in a short span. The signal threshold for target detection is 2.6. The window size w=500 and error_threshold=0.1.

5.2 Results and Analysis

Table 4 shows the SRUTL algorithm addressing various security attacks at different levels. The network performance is evaluated in terms of success probability at all 3 groups of nodes i.e., cluster members, cluster decoders and cluster heads.

Table 4. SRUTL Algorithm and its Defense to Various Attacks at Different Levels

Security Attacks	Bad Mouth Attack	Sybil Attack	On-off Attack	Malicious Node Attack
Phase 1			CMs	CMs
Phase 2	CDs	CDs		CDs
Phase 3			CHs	CHs

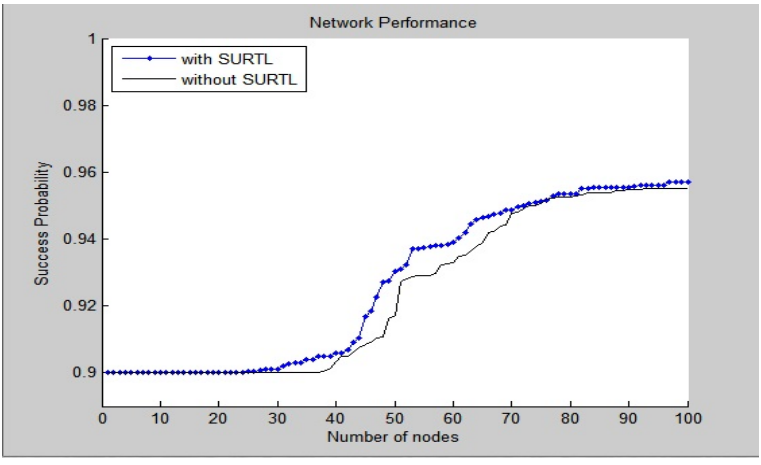

Fig. 1. Network Performance with SRUTL algorithm

The Figure 1 show the number of nodes contributing in solving ATL problem is defended by the use of SRUTL algorithm. This is due to filtering of faulty nodes in 3 phases and different levels of target location estimation process. The use of stability factor along with reputation value has shown positive results in identifying malicious nodes and other attacks.

6 Conclusions and Future Work

The proposed SRUTL algorithm presents a simple and effective security framework for WSNs. The results show a high overall performance when compared with the network without this algorithm. The energy efficiency and high accuracy adds to its advantage. With reputation update better target localization is performed. The various node attacks considered viz., bad-mouth attack, Sybil attack, on-off attack and malicious nodes are detected at earlier stages, so that network remains stable and unaffected. The special cases of nodes failing at cluster head level are not addressed and hence would be continued in our future works. Simulation results show that SRUTL can successfully overcome various attacks at different levels of the algorithm for target localization using reputation.

References

1. Zaher, M.M., Mohamed, A.E., Magdy, A.B.: A Lightweight Collaborative Fault Tolerant Target Localization System for Wireless Sensor Networks. IEEE Transactions on Mobile Computing 8(12), 1690–1704 (2009)
2. Zhong, Z., Zheng, P., Jun-Hong, C., Zhijie, S., Amvrossios, C.B.: Scalable Localization with Mobility Prediction for Underwater Sensor Networks. IEEE Transactions on Mobile Computing 10(3), 335–348 (2011)

3. Alexander, T.I., John, W.F., Randolph, L.M., Alan, S.W.: Nonparameteric Belief Propagation for Self-Localization of Sensor Networks. IEEE Journal on Selected Areas in Communications 23(4), 809–819 (2005)
4. Ozdemir, O., Niu, R., Pramod, K.V.: Channel Aware Target Localization with Quantized Data in Wireless Sensor Networks. IEEE Transactions on Signal Processing 57(3), 1190–1202 (2009)
5. Amitangshu, P.: Localization Algorithms in Wireless Sensor Networks: Current Approaches and Future Challenges. Network Protocols and Algorithms 2(1), 45–74 (2010) ISSN 1943-3581
6. Xue, W., Dao-wei, B., Liang, D., Sheng, W.: Agent Collaborative Target Localization and Classification in Wireless Sensor Networks. Sensors, 1359–1386 (2007), ISSN 1424-8220, http://www.mdpi.org/sensors
7. Raghavendra, V.K., Venayagamoorthy, G.K., Ann, M., Cihan, H.D.: Networkcentric Localization in MANETs based on Particle Swarm Optimization. In: IEEE Swarm Intelligence Symposium, St. Louis, MO, USA (2008)
8. Xu, L., Zhang, H., Shi, W.: Mobile Anchor Assisted Node Localization in Sensor Networks based on Particle Swarm Optimization. In: IEEE Conferences (2010)
9. Panigrahi, T., Panda, G., Mulgrew, B., Majhi, B.: Maximum Likelihood Source Localization in Wireless Sensor Networks Using Particle Swarm Optimization. In: IEEE ICES, pp. 111–115 (2011)
10. Xue, W., Liang, D., Daowei, B.: Reputation-Enabled Self-Modification for Target Sensing in Wireless Sensor Networks. IEEE Transactions on Instrumentation and Measurement 59(1) (2010)