iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 Issue: VII Month of publication: July 2021

DOI: https://doi.org/10.22214/ijraset.2021.36685

Trust Based Approach to Counter Attacks on WSN

Palak Garg[1], Prakhar Gaur[2], Saumya Acharya[3], Ranjit Kumar[4], Javed Miya[5], Suresh Kumar[6]
[1, 2, 3, 4, 5, 6]Galgotia College of Engineering And Technology

Abstract: Wireless sensor networks (WSN) have a developing future due to their minimal expense, power-efficiency, and simple to-carry out attributes. Be that as it may, its security issues have become an interesting issue of exploration these days.

This article inspects the headway of system of countering assaults where the responsibility, leftover energy of hub and examination of effective and fruitless occasions are consider while registering the trust level. Unlike existing work, this paper talk about the technique in which the trust esteem per layer of a sensor hub is assessed by the deviations of key boundaries at every convention layer considering the attacks. The execution of the proposed counter measure is then investigated utilizing the t-conveyance. Reproduction of WSN has been done to approve the outcomes. With the assistance of reenactment results, it has been seen that the proposed trust-based methodology for interruption location beats existing plans to the extent of revealing safety breaks in WSN.

Keywords: Wireless Sensor Network, , intrusion detection, trust value

I. INTRODUCTION

Remote sensor organizations (WSN) are a multi-jump impermanent self-sufficient framework comprised of a gathering of versatile hubs with remote transmitters and receivers. Wireless sensor organizations (WSNs) are generally utilized in assortment of fields, for example, farming, ecological, mechanical and military observing applications. Security guaranteeing is one of the significant issues at arrangement and activity of WSN. wireless sensor networks are powerless against different kinds of assaults, including Sybil, Wormhole, Black-opening, Gray-opening, Hello Flood, and Distributed Denial of Service assaults.

According to the analysis of attacks in WSN, most of the attacks are active . Active attacks can cause a deconstructive impact on WSN and cause an entire or partial network downtime. It is generally agreed that the intrusion detection system and trust management are the most widely used at counteraction of active attacks.

WSNs face serious security problems, due to the openness of nodal deployment and wireless communication. In some WSN deployments, the SNs could also be captured and therefore the key information could be leaked or compromised. The purpose of an attacker is to disrupt the safety attributes of WSNs, including confidentiality, integrity, availability and authentication. To achieve this the attacker may target various protocol layers. Considering the limited resources of the SNs, it's not realistic for WSNs to implement high-strength security mechanisms.

Besides, the attacker may surpass the security check of WSN with the advancement in technologies. Intrusion detection schemes serve as a second wall and play an important role in controlling the attacks .The intrusion detection system for WSNs can detect whether there are behaviors violating the safety policy and record evidence of being attacked by collecting and analyzing the knowledge from sensor nodes and networks. It can send an alarm timely to the supervisor and perform some countermeasures against the attack.

We have put forward an approach to counter attacks in WSN through this paper. The developed method considered that the attacks will surely affect the various parameters of the protocol layer that's why it uses the deviations of parameters of different protocol layers to calculate trust . Beside the above advantages there is one more benefit of the developed method - when unsuccessful events occur in the network , it is capable of detecting the attacker.

This paper follows the following format- Section 2 (Related Work) contains a survey of existing work on intrusion detection based on trust , Section 3 (Proposed Work) has a detailed description of the approach we have put forward ,Section 4 (Simulation Result) this section gives validation to the presented approach based on the simulation result and comparison with the existing methods, Section 5 (Conclusion), Section 6 (References).

II. RELATED WORKS

Trust management is an effective method to identify malicious nodes. As of late, research on trust based interruption recognition has gotten extensive consideration from scientists. The current plans mean to further develop the location execution, asset proficiency, and energy effectiveness and so forth, by utilizing fuzzy theory, weighting methods, etc.

The work on dependable, trust-based, and energy-proficient convention for remote sensor networks is introduced in . The iRTEDA convention consolidates the standing, leftover energy, interface accessibility, and a recuperation component to improve secure information conglomeration and ensure that the organization is secure, dependable, and energy-effective. This convention utilizes a standing capacity that depends on a Beta circulation to evaluate the standing and reliability of hubs. The data concerning the residue energy and connection accessibility of the hubs was updated to help the organization to reselect aggregators and work on the power of the picked directing way, when the aggregators are decided as compromised hubs. This convention depends on the trust estimation technique proposed in reference , which shows the RFSN framework, which depends on Bayes' hypothesis and beta-appropriation. The main idea of iRTEDA protocol which makes it different from others is that - residual energy and availability must be considered to select nodes for routing packets and trust value only is not sufficient to do that. The main flaw of the above approach is that the attacker can have availability to large energy resources thus can establish a high trust value and will be able to avoid any unsuccessful event and will be considered as a non malicious node. Beside this a lot of energy is consumed by network nodes to continue the flow of information and availability of nodes due to which the cost to maintain security gets hiked up.

III. PROPOSED WORK

The introduced trust assessment technique involves the assurance of concentrated and direct trust estimates. The main thing about this technique is the first method of deciding the unified trust esteem. The worth is determined by the CH as opposed to adjoining hubs which will bring down the worth of correspondence among hubs and the computational burden. This strategy incorporates investigating probabilities with which the heap L and consequently the remaining energy Q (E) of the hub fall during a foreordained certainty stretch. This certainty span is determined for a gaggle of organization hubs inside the current stretch . The likelihood of falling into the pomposity span permits assessment, surpassing the current hub at the very pinnacle of or least suitable worth. This correlation permits distinguishing dynamic assaults like refusal of administration, flooding parcels, assaults coordinated with exhaustion of assets. And furthermore it's anything but a gatecrasher on the off chance that it has more noteworthy energy assets than different SNs. The tactic involves two steps:-

A. Calculation Of Direct Trust

The trust of each node includes the trust value of different protocol layers.

In our proposed approach we have considered only physical and network layer trust as these layers are on target for most attacks. It can be calculated by:

$$T_{ij\ direct}(t) = W_1 T_{ij\ physical}\ (t) + W_2 T_{ij\ network}\ (t)$$

where Tij direct(t) is the direct trust value of a node which is evaluated against its neighboring node j at time t.

The reliability of a SN (or CH) should be upgraded periodically. Node i estimates the trust of node j throughout a time window of length Δt, so the upgrade trust of node i in connection with node j is:

$$T_{ij}(t) = T_{ij}(t - \Delta t) + T_{ij\ direct}\ (t) + T_{ij\ centralized}\ (t)$$

where T_{ij}(t − Δt) denotes the historical trust value of node i toward node j.

B. Calculation Physical Trust

Energy consumption rate is a key framework at the physical layer. A malicious node ordinarily sends or receives more packets compared to a normal node. It will inescapably consume high node energy, so we select energy consumption as a trust metric at this layer. The monitoring node 'i' can achieve the energy consumption of its neighboring node j all over the time period of Δt. The relative deviation of energy consumption of node j can be calculated by:

RD_{EC}(t) = ΔE_j(t) − $\underline{\Delta E(t)}$

ΔE(t)

The higher the deviation of energy consumption is, the lesser the nodal trustworthiness will be. So we obtain the physical layer of trust as:

$T_{ij\ phy}$(t) = 1 − RD_{EC}(t), if 0 < RD_{EC}(t) < 1
0 , RD_{EC}(t) ≥ 1
1 , RD_{EC}(t) ≤ 0

C. Calculation Of Network Trust

Attacks at the network layer focus on derange network routing, and receive the data flows. A malicious node can shape itself a part of a routing path by exhibiting bogus routing messages, such as a good Link Quality Indicator (LQI) or a small hop count. It can also begin selective or sinkhole forwarding attacks and result in releasing every or some part of forwarding packets. Therefore, we pick route metrics as well as packet forwarding rate as trust metrics to estimate the network layer trust. The network layer trust is described as:

$$T_{ij\ net}(t) = q1T_{ij\ route\ metric}(t) + q2T_{ij\ pfr}(t)$$

D. Calculation Of Centralized Trust

1) The CN calls the worth of leftover energy just as the worth of burden (the aggregate sum of traffic passing across the hub).
2) We use the typical distribution for the heap L and the leftover energy Q(E) for computing certainty spans and trust esteem.
3) The CH (BS) sets up the class limit for typical dissemination for leftover energy and hub load.
4) CN computes the lower furthest reaches of certainty span for leftover energy and as far as possible for hub load :

$$a_{min} = \underline{Q(E)} - t.\sigma_{Q(E)}/\sqrt{n}$$
$$a_{max} = E_{max}$$
$$b_{min} = L_{min}$$
$$b_{max} = \underline{L} + t.\sigma_L/\sqrt{n}$$

where t*$\sigma/\sqrt{n}$ is the estimation accuracy, t is the argument of the Laplace function where $\phi(t) = \alpha/2$, α is the defined reliability, σ_L-standard deviation for load, $\sigma_{Q(E)}$ - standard deviation for residual energy.

5. Further CN estimates the probability of hitting the current value of load P_L and residual energy $P_{Q(E)}$, values for the sample of the mathematical expectation in the confidence interval for each node

$P_{Q(E)}(a_{min} < Q(E) < a_{max}) = \phi((a_{max} - \underline{Q(E)})/\sigma_{Q(E)})$ - $\phi((a_{min} - \underline{Q(E)})/\sigma_{Q(E)}$

$P_L(b_{min} < L < b_{max}) = \phi((b_{max} - \underline{L})/\sigma_L$ -
$\phi((b_{min} - \underline{L})/\sigma_L)$

If Tcent>5then the node will be considered as trusted.
If Tcent = 0,5, then the node will be considered uncertain.
If Tcent < 0,5, then the node will be considered untrusted.

IV. SIMULATION RESULTS

A Wireless sensor network of 100 nodes was set up using a MATLAB simulator.

The below table 1 contains values of different parameters used in the simulation of the network.

Nodes are placed randomly and can change their location. The simulated network has been tested against various types of attacks such as sybil attack,denial of service attack,grey-hole attack,black hole attack

The following parameters were used to determine the effectiveness:

1) Ability of the nodes to perform efficiently, regardless of what the surrounding conditions are or when nodes are being targeted by attacks.
2) Accuracy of the trusted / non-trusted node indicates its coincidence with the truth value of the measured value.

Table i. Network simulation details

The number of nodes in the network, k	100
Simulation time	300(sec)
The trust level computation interval	10
The initial energy level, J	30
Transmitter power, mW	0,4
Routing protocol	AODV
Data transfer protocol	UDP

Table II. Comparison to counter attacks

Attack	Trust Management Type			
	RFSN	*LTDS*	*BTMS*	*PROPOSED*
Black Hole	m	m	m	m
Gray Hole	m	m	m	m
Sybil	x	m	x	x
Denial Of Service	x	x	m	m
Wormhole	m	m	m	m

"m" identifies malicious nodes , "x" does not identify a malicious node. The advantage of the proposed method is the detection of the breach in wsn even when the failed events do not take place . This benefit comes by the computation method of the centralized trust value. It is shown by experiments that despite the fact that the node successfully performs its functions in the process of packet forwarding, it is capable of carrying out an attack on the depletion of node resources, or collecting data about the system for personal advantages. For instance, when trust factors, and cross-layer attacks are rarely taken into account. To spot an attacker who realizes the Sybil attack, the attacker introduces multiple objects, networks and redirects all the routes for themselves, which results in intercepting the original information.

V. CONCLUSION

There exist various types of attacks which target various protocol layers of wsn. In the existing trust-based countermeasures there is no unified standard to pick malicious nodes more efficiently. We've put forward a protocol layer trust-based approach for countermeasures of attacks in WSNs. In our proposed method, we compare various parameters of different protocol layers and direct and centralized trust value is calculated and the trust values of nodes are calculated according to deviation of parameter. By comparing the trust value with standard values , we label the node as malicious or non-malicious

REFERENCES

[1] Wood, A.D.; Stankvic, J.A. Denial of service in sensor networks. IEEE Comput. 2002, 35, 54–62. [CrossRef]

[2] Lira, A.T.H.; Lau, H.K.; Timmis, J.; Bate, I. Immune-inspired self healing in wireless sensor networks. In Proceedings of the 11th International Conference on Artificial Immune Systems, Taormina, Italy, 28–31 August 2012; Volume 7597, pp. 42–56.

[3] Feng, R.; Xu, X.; Zhou, X.; Wan, J. A trust evaluation algorithm for wireless sensor networks based on node behaviors and d-s evidence theory. Sensors 2011, 11, 1345–1360. [CrossRef] [PubMed]

[4] Atakli, I.M.; Hu, H.; Chen, Y.; Ku, W.S.; Su, Z. Malicious node detection in wireless sensor networks using weighted trust evaluation. In Proceedings of the Symposium on Simulation of Systems Security, Ottawa, ON, Canada, 14–17 April 2008; pp. 836–843.

[5] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava. "Reputation based framework for high integrity sensor networks" ACM Trans. Sen. Netw., vol.4, no. 3, 2008. pp. 1-37

[6] Bjorn Stelte and Andreas Matheus. "Secure Trust Reputation with Multi-Criteria Decision Making for Wireless Sensor Networks Data Aggregation". IEEE Transaction on Network and Service Management, 2011, pp. 920 – 923

[7] Woo, A.; Tong, T.; Culler, D. Taming the Underlying Challenges of Reliable Multihop Routing in Sensor Networks. In Proceedings of the 1st International Conference on Embedded networked sensor systems (SenSys), Los Angeles, CA, USA, 5–7 November 2003; pp. 14–27.