ISSN 2394-739X
International Journal for Research in Science Engineering and Technology

LOCATION AWARE SENSOR ROUTING PROTOCOL FOR DETECTING MALCIOUS NODE IN WIRELESS SENSOR NETWORK

[1]V.DIVYA, [2]Prof. R.VISWANATHAN.,M.Sc.,,
[1]M.PHIL RESEARCH SCHOLAR, [2]M.Phil.,,
[1,2]PG&RESEARCH DEPT OF CS,
[1,2]MUTHURANGAM GOVT ARTS COLLEGE (AUTONOMOUS),
[1,2]VELLORE.

ABSTRACT

Wireless Sensor Network (WSN) is the developing and testing technology with low preparing and battery control. Security turns into a noteworthy issue in WSN as a result of its wireless nature it is inclined to different sorts of attacks and losing of information bundle. Our plan gives a mechanism to creating notoriety and trust with the goal that a gadget can decide if different gadgets have been traded off, and make remedial move, through negative information sharing and independent trust-based decision making. We additionally introduce a simple location verification algorithm that uses got flag quality information in the verification of detailed location information. The adequacy of our way to deal with recognizes and disconnect bargain nodes is approved through reproduction. The outcomes demonstrate that our simple location verification algorithm gives a viable mechanism to the detection and isolation of traded off non-colluding and colluding nodes.

Keywords: [Probability, Colluding, Protocol, Wireless Sensor, Location Verification]

1. INTRODUCTION

Wireless sensor networks (WSN) are accumulation of nodes where every hub has its own sensor, processor, Transmitter and receiver. The sensors are minimal effort gadgets that play out a particular sort of detecting occasion. Being of ease such sensors are conveyed thickly throughout the zone to screen particular occasion. WSN are exceptionally distributed networks of little lightweight wireless nodes. Sensor nodes are called as bit. It screens nature or framework by measuring physical parameters, for example, temperature, weight, stickiness and so forth. Sensor networks are generally connected in different recorded, for example, condition checking, military applications, medicinal services and home insight. For monetary feasibility, sensors nodes are constrained in power, computation capabilities and memory. The impediment of memory and preparing capacity makes public key cryptography and digital signature infeasible. Also, the constrained power of these minor sensor nodes makes the correspondence overhead of customary security algorithm horrendous. Moreover, the absence of framework, the uncertain idea of wireless correspondence channel, and threatening organization situations introduce extra security vulnerabilities.

We display a localized protocol, which mitigates inward assault through trust based decision making. We utilize location mindfulness, a typical element of numerous sensor network applications, and got flag quality in the approval of location information. Our reputation based trust display is dynamic, that is, trust measurements are always being invigorated. Reputation in our work is a probabilistic dissemination comparable in nature as established. Basic to our approach is the capacity of nodes to screen the movement going all through their neighbors. Consider 1 spoke to along with graph of wireless sensor network.

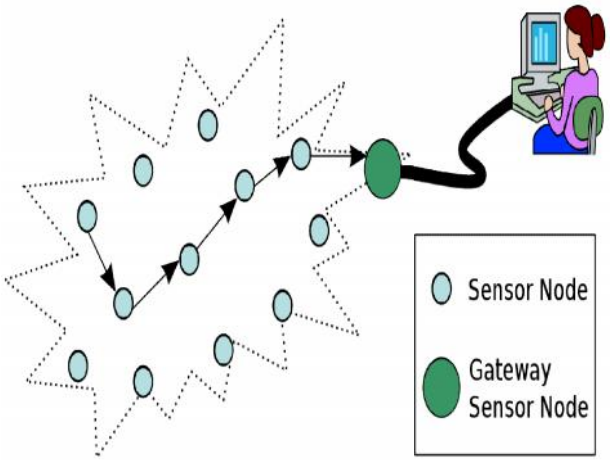

Figure 1: Wireless Sensor Network

We utilize an information structure that stores the trust esteems in a trust table kept up by every hub. Every hub constructs and keeps up its trust table by observing its neighbors. The oddity lies in our approach of independent evaluation and trust based decision endless supply of negative information identifying with potential isolation of compromised nodes; and the incorporation of location mindfulness as a circuitous component in trust building. Our commitments are (I) resilience to hub compromise-our plan offers reputation based checking that encourages the detection and isolation of untrustworthy nodes and (ii) location mindfulness we coordinate location mindfulness in our reputation based plan to upgrade the honesty. We additionally present a simple plan that utilizations got flag quality to check the location information.

2. LITERATURE REVIEW

Chakraborty, et al. tended to the issue of malignant foes in WSN through three layered trust based engineering. The proposed approach separates lawful and illicit sensor nodes and sift through produced and beguiling information. Notwithstanding, this approach is without observing mechanism and for overseeing mystery key it require some additional computation and capacity. Theodore, et al. proposed a trust mindful location based directing protocol named ATSR (A Trust Aware Routing Protocol). It ensure network with noxious nodes and bolster extensive scale nodes sending. In this approach the nodes screen neighboring hub conduct and assess trustworthiness before sending. This protocol likewise consider circuitous or reputation trust information and immediate and backhanded information converged to compute add up to trust and geological information.

T. Zahariadis, P. Trakadas, H. C. Leligou, S. Maniatis, and P. Karkazis proposed a trust model and consolidate every hub immediate and backhanded trust information to characterize the trustworthiness of all its one bounce separate neighbors. The proposed ATSR protocol receives location based way to deal with lessen handling, stockpiling. Protocol performed on bounce by-jump premise and next expectation choice based on adjusting of steering and security criteria. Creator asserted that his proposed display uncovers malignant nodes despite the fact that with various attacks and characterizes elective trust based course to the goal. In any case, on account of high portability of nodes this approach sets aside time for setting up trust between nodes.

Y. Reddy and R. Selmic suggested that trust based approach creator utilized rehashed diversions for detection noxious nodes. The part of rehashed diversion methodology in wireless sensor network

computed the normal number of dropped parcels verses rebate result. The model is valuable to exchange the bundles with least overhead. Fundamentally the diversion hypothesis is a bi-directional and WSN is a restricted transmission where sensor nodes send the information to base station. In this circumstance this approach isn't useful in view of non-prescient nature of wireless network.

Zhou et al proposed a trust mindful and location based secure steering protocol to ensure the WSN against directing attacks. This protocol was stretched out from GPRS protocol consolidates the security mechanism.

Ahvar et al examined the fluffy based vitality mindful steering protocol for WSN. Dread protocol considers the vitality adjusting and vitality sparing. A reasonable exchange off was ascertained between vitality adjusting and vitality sparing based on the fluffy set idea.

3. PROPOSED WORK

3.1 Location Verfication Algorithm

We accept that our nodes know about their location. To accomplish this, by and large two methodologies are utilized: range-free and range-based. While we perceive the preferences and burdens of the two 16 approaches we trust that any of these, appropriately adjusted, can be utilized in our model. In any case, for accommodation, we expect that every hub can decide its precise location. In any case, their strategy does not check precise location yet rather if a hub is inside the district it guaranteed. Likewise, the nodes must have the capacity to impart utilizing both radio recurrence and sound (regularly ultrasound frequencies). Our protocol varies in that we additionally confine the location potential outcomes to a restricted locale along a concentric circle. Notwithstanding location mindfulness, we accept that an appropriation of got signal strength variation is known an earlier, and that it is uniform. Further to this we accept that the standard deviation of the dispersion has been registered already. Later we will clarify the explanations behind the presumptions of the standard deviation and the known circulation of the got signal. At long last, all parameters identifying with the way misfortune demonstrate are expected known. Our protocol means to approve location information as opposed to identify nodes that intentionally report adulterated location information. Nonetheless, through our approval procedure, nodes that distort location information can be identified and secluded. Figure 2 and 3 spoke to into abnormal state and detail depiction of location verification algorithm.

Request location information using randomly generated nonce for freshness
If response is received decrypt message to obtain location
Compute expected location (distance) based on the received signal strength (RSS) and the Free Space Propagation path loss model
If (distance obtained) minus (distance computed) differs by a value greater than the threshold
Blacklist s_j
Else return location confirmed;
End;

Figure 2: High Level Description of Location Verification Algorithm

//Request location using randomly generated nonce for freshness
$s_i \rightarrow s_j : N_i$
// Reply with location
$s_j \rightarrow s_i : K_s\{ID_j | XY_j | MAC_{K_s}(ID_j | N_i | XY_j)\}$
//Compute location based on RSS and Free Space Propagation path loss model
$s_i : d = \sqrt{\frac{P_t G_t G_r \lambda^2}{(4\pi)^2 L}}$
// Check if distance obtained minus distance computed differs by a value greater than the threshold
If $s_i : |(XY_i - XY_j)| - d| > \delta$
Blacklist s_j
Else return location confirmed;
End.

Notation:
// Where d is the distance between transmitting node and receiving node ; G_t, G_r, and L are constant
// parameters of the transceiver; λ is the wavelength of the communication signal; P_t is the transmitting
// power and π is a constant.
// δ is the standard deviation of the RSS distribution.

Figure 3: Detail Description of Location Verification Algorithm

4. EXPERIMENTAL RESULTS

We have characterized four sorts of nodes: great, awful, colluding and irregular. Great nodes are set to have parcel drop rate that is under 15 %. Terrible nodes have bundle drop rate of 85% or more noteworthy. Colluding nodes are terrible nodes that have

under 15% parcel drop rate among themselves, and more noteworthy than 85% with other non-colluding nodes, regardless of whether these non-colluding nodes are great or awful. We utilize a simple message trade protocol where every hub arbitrarily sends message to any nodes in its neighbor list that isn't boycotted.

Simulation Round

Figure 4 exhibits the connection between the Average Percentage Drop Packet and Average Trust for the neighbors of an awful hub. At first, we see that the average slow increment at that point quickly increment to right around 100%. We clarify this pattern as takes after: at the beginning the nodes collaborate with the compromised hub however, as its neighbors record its activities and figure its trust level they start a procedure of boycotting, this takes a short period before essentially every one of the nodes in the group boycotts this hub.

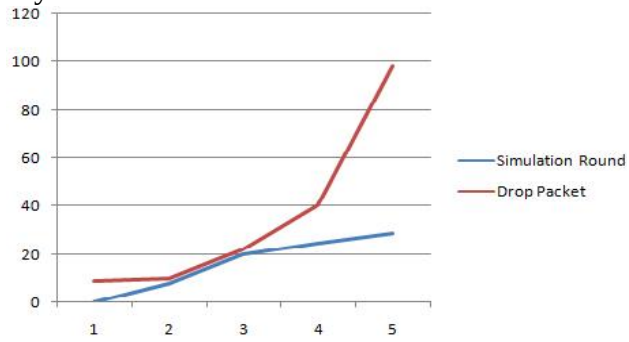

Figure 4: Average Percentage Drop Packet versus Simulation Round of Bad Node

Probability of Blacklisting

We set up an alternate trial to examine the capacity of the protocol to separate compromise nodes. We set 5% of the nodes to be awful while the others are great. No colluding are arbitrary nodes are incorporated. We deliberately increment the quantity of nodes in augmentations of 5 from 0 to 60. We utilize similar information trade protocol as earlier and the information rate was set to 2 Mb/s. Parcel lengths are 10kbit and are created every one moment.

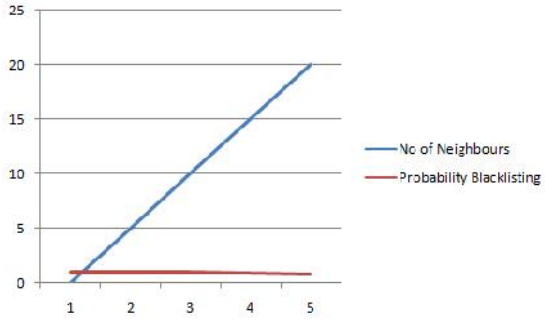

Figure 5: Probability of Compromised Node Isolation by more than 40% of neighbors

Figure 5shows that the likelihood for compromised hub detection is sure when the quantity of neighboring nodes is 15 or less. As the quantity of neighboring nodes 25 expands, the likelihood of boycotting by over 40% of the neighboring nodes diminishes. This is because of expanding impact of parcel as the thickness of the group increments. This impact causes an expansion in false positives by the checking nodes.

Percentage of Colluding Nodes

Figure 6 demonstrates that this likelihood is 1 for a relative little level of colluding nodes however; it diminishes exponentially and approaches 0 with additionally increment in the level of colluding nodes. This happens in light of the fact that it turns out to be progressively troublesome for a decent hub to spread negative information that outcomes in the isolation of compromised colluding nodes within the sight of an expanding level of colluding nodes. This is because of the amassing of distorted revealing by the colluding nodes.

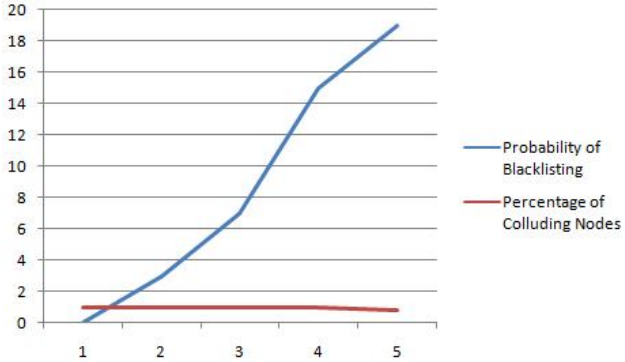

Figure 6: Probability of Blacklisting Colluding Nodes by 40% of Neighbors

CONCLUSION

We have introduced a location mindful trust based localized protocol that can identify and detach compromised or pernicious nodes. We utilize a Location Verification Algorithm. Our algorithm is plan with regards to a group based network show with nodes that have special nearby IDs. We present a simple location verification algorithm that validates announced location information. Our algorithm is surveyed by its capacity to identify and disengage compromised nodes. Recreations show that our protocol effectively distinguishes and disengage compromised nodes even within the sight of colluding nodes.

REFERENCES

[1] A. Chakraborty, V. Parekh, and A. Ruia, "A Trust Based Routing Scheme for Wireless Sensor Networks," in Advances in Computer Science and Information Technology. Networks and Communications, ed: Springer, 2012, pp. 159-169.

[2] T. Zahariadis, H. Leligou, P. Karkazis, P. Trakadas, I. Papaefstathiou, C. Vangelatos, et al., "Design and implementation of a trustaware routing protocol for large wsns," International Journal of Network Security & Its Applications (IJNSA), vol. 2, pp. 52-68, 2010.

[3] T. Zahariadis, P. Trakadas, H. C. Leligou, S. Maniatis, and P. Karkazis, "A novel trust-aware geographical routing scheme for wireless sensor networks," Wireless personal communications, vol. 69, pp. 805-826, 2013.

[4] Y. Reddy and R. Selmic, "A Trust-based Approach for Secure Packet Transfer in Wireless Sensor Networks," International Journal On Advances in Security, vol. 4, pp. 198-207, 2012.

[5] Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Ad Hoc Networks, 1, 293–315.

[6] Momani, M. and Challa, S. (2010). Survey of Trust Models in Different Network Domains. IJASUC, 1(3), pp.1-19.

[7] Bin, T.,Xian,Y.Y., Dong, L.,Qi, L.,&Xin,Y. (2010).A security framework for wireless sensor networks. The Journal of China Universities of Posts and Telecommunications, 17, 118–122.

[8] Zhang,Y.,Yang, J.,Li,W.,Wang, L.,&Jin, L. (2010).An authentication scheme for locating compromised sensor nodes in WSNs. Journal of Network and Computer Applications, 33, 50–62.

[9] Bellare M, Micciancio D. A new paradigm for collision-free hashing: incrementality at reduced cost. In: Eurocrypt'97, Lecture notes in computer science, vol. 1233, 1997.

[10] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, July 1982.

[11] Haiyun Luo, Petros Zerfos, Jiejun Kong, Songwu Lu, Lixia Zhang, "Self-securing Ad Hoc Wireless Networks," IEEE ISCC (IEEE Symposium on Computers and Communications) 2002, Italy.

[12] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis and Defense," International Symposium on Information Processing in Sensor Networks, Vol. 1(2004).

[13] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar, "SPINS: Security Protocols for Sensor Networks, 7th Annual International Conference on Mobile Computing and Networking (MobiCom 2001), 2001.

[14] Chris Karlof , Naveen Sastry, David Wagner "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks" SenSys'04, November 3–5, 2004, Baltimore, Maryland, USA

[15] HangRok Lee, YongJe Choi, HoWon Kim "Implementation of TinyHash based on Hash Algorithm for Sensor Network". World Academy of Science, Engineering and Technology, Vol. 10, 2005.

[16] Matthias Becker, Sven Schaust and Eugen Wittmann. Performance of Routing Protocols for Real Wireless Sensor Networks. 10th Int. Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS'07), San Diego, USA, 2007.