International Journal of Research
Available at https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October2016

Privacy preserving and the detection of the packet networks when the attacks fail in the wireless sensor networks

S.Ramana Reddy, Mr. B. Mahender Reddy

Abstract—

These are characterized by long periods of disconnected operation and fixed or irregular intervals between sink visits. The absence of an online trusted third party implies that existing WSN trust management schemes are not applicable to WSNs. In this paper, we propose a trust management scheme for WSNs to provide efficient and robust trust data storage and trust generation. For trust data storage, we employ a geographic hash table to identify storage nodes and to significantly decrease storage cost. We use subjective logic based consensus techniques to mitigate trust fluctuations caused by environmental factors. We exploit a set of trust similarity functions to detect trust outliers and to sustain trust pollution attacks. We demonstrate, through extensive analyses and simulations, that the proposed scheme is efficient, robust and scalable.

1 INTRODUCTION

In this paper, while watching an arrangement of bundle misfortunes in the system, we are occupied with figuring out if the misfortunes are brought about by connection mistakes just, or by the joined impact of connection blunders and pernicious drop. We are particularly intrigued by the insider-assault case, whereby noxious hubs that are a piece of the course abuse their insight into the correspondence connection to specifically drop a little measure of parcels basic to the system execution. Since the parcel dropping rate for this situation is practically identical to the channel mistake rate, routine calculations that depend on distinguishing the bundle misfortune rate can't accomplish palatable identification precision. To enhance the discovery precision, we propose to abuse the connections between's lost parcels. Besides, to guarantee honest estimation of these connections, we build up a homomorphic direct authenticator (HLA) based open examining design that permits the identifier to confirm the honesty of the parcel misfortune data reported by hubs.

II. OBJECTIVE AND SCOPE OF THE PROJECT

Our proposed project concentrates on securing the network from the malicious attack. Our implementation results in the efficient detection and elimination of vampire attack from the network. In order to detect and eliminating the vampire attack we going to implement certain intrusion detection system based on the energy level constraints. Our simulation result shows the improved network authentication rate and efficient detection of malicious node from the network, so that our proposed system forms a secure network with high throughput rate.

III. EXISTING SYSTEM

In the existing system the trust management scheme for efficient trust generation as well as scalable and robust trust data storage in WSNs. A central issue for trust management in WSNs is how to store trust data without relying on a trusted third party. Initially, we consider two simple trust management schemes as a first-step attempt to address the existing trust storage problems in WSNs. Our advanced scheme allows sensor nodes to put and get trust data to and from designated storage nodes based on node IDs. Sensor nodes do not need to know the IDs of storage nodes. They use a hash function to find locations of the storage nodes, which significantly reduce the storage cost. We also propose a set of similarity threshold functions to remove outliers from trust opinions. This prevents attackers from generating false trust opinions and from polluting trustworthiness.

Disadvantages The presence of vampire attack in the network will permanently disable the whole network. The energy level of nodes tends to 0 joules because of vampire attack presence. This system doesn't concentrates on eliminating the vampire attacks

IV. PROPOSED SYSTEM

The proposed system concentrates on a secure data transmission from the adversary nodes in the sensor network. In order to build a secure network, the network should be an extinct to adversary nodes. So we propose a technique called nodes position verification and node verification intrusion detection techniques [IDS]. The nodes which has the exceed threshold value other than normal nodes, then a node supposed to be a malicious nodes which will undergoes a vampire attack. By the proposed IDS system we can calculate the threshold value and energy level of malicious nodes, and also by NPA techniques the malicious nodes can be detected efficiently and detected nodes are eliminated from the network which increases the network performance ant throughput rate.

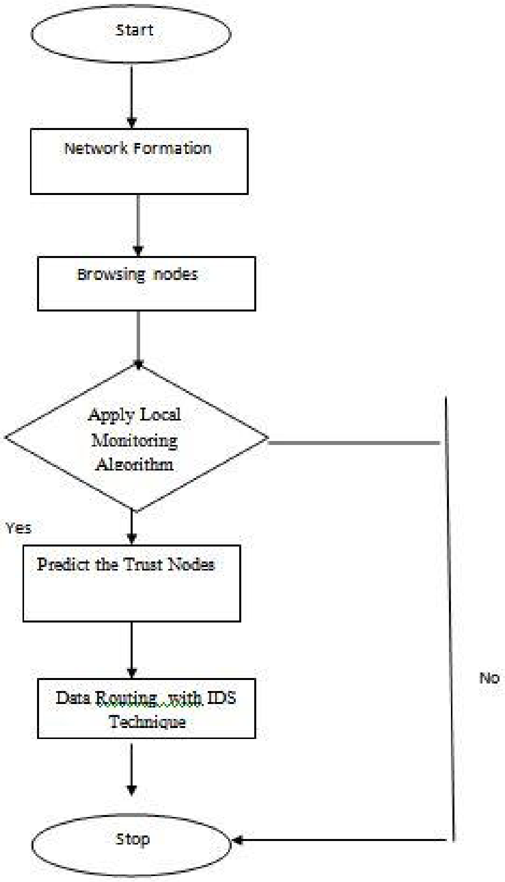
Advantages

□ Developing an analytical model for intrusion detection in WSNs, and mathematically analyzing the detection probability with respect to various network parameters such as node density and sensing range.

□ Applying the analytical model to single-sensing detection and multiple-sensing detection scenarios for homogeneous and heterogeneous WSNs.

□ . Defining and examining the network connectivity and broadcast reachability in a heterogeneous WSN we derive the expected intrusion distance and evaluate the detection probability in different application scenarios. Given a maximal allowable intrusion distance Dmax =E, we theoretically capture the impact on the detection probability in terms of different network parameters, including node density, sensing range, and transmission range. For example, given an expected detection distance E(D), we can derive the node density with respect to sensors' sensing range, thereby knowing the

V. FLOWCHART



VI. MODULES DESCRIPTION

NODE CONFIGURATION SETTING

The mobile nodes are designed and

configured dynamically, designed to employ across the network, the nodes are set according to the X, Y, Z dimension, which the nodes have the direct transmission range to all other nodes. **DATA ROUTING** The source and destination are set at larger distance, the source transmits the data packets to destination through the intermediate hop nodes using UDP user data gram protocol, link state routing like PLGP act as an ad hoc routing protocol.

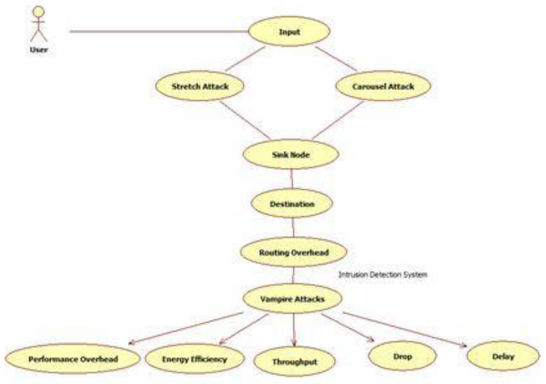
NODES UNIQUE IDENTITY

All the mobile nodes tend to have a unique id for its identification process, since the mobile nodes communicates with other nodes through its own network id. If any mobile node opted out of the network then the particular node should surrender its network id to the head node.

HOP-BY-HOPMESSAGE AUTHENTICATION

Every forwarder on the routing path should be able to verify the authenticity and integrity of the messages upon reception. This can be done through the verification of public key. ACK is replied to previous hop node if authentication is successful. **CAROUSEL ATTACK** In this Carousel attack, an adversary sends a packet with a route composed as a series of loops, such that the same node appears in the route many times. This strategy can be used to increase the route length beyond the number of nodes in the network, only limited by the number of allowed entries in the source route. An example of this type of route is in Fig.1.1, malicious node 0 carries out a carousel attack, sending a single message to node 19 (which does not have to be malicious).Note the drastic increase in energy usage along the original path. Assuming the adversary limits the transmission rate to avoid saturating the network, the theoretical limit of this attack is an energy usage increase factor is the maximum route length. Overall energy consumption increases by up to a factor of 3.96 per message. On average, a randomly located carousel attacker in our example topology can increase network energy consumption byafactorof1:48 0:99.The reason for this large standard deviation is that the attack does not always increase energy usage the length of the adversarial path is a multiple of the honest path, which is in turn, affected by the position of the adversary in relation to the destination, so the adversary’s position is important to the success of this attack.

VII. SYSTEM ARCHITECTURE:



VIII. CONCLUSION

We defined Vampire attacks, a new class of resource consumption attacks that use routing protocols to permanently disable ad-hoc wireless sensor networks by depleting nodes' battery power. These attacks do not depend on particular protocols or implementations, but rather expose vulnerabilities in a number of popular protocol classes. We showed a number of proof-of-concept attacks against representative examples of existing routing protocols using a small number of weak adversaries, and measured their attack success on a randomly-generated topology of 30 nodes.

REFERENCE

[1] J. N. Arauz, 802.11 Markov channel modeling, 2004

C. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable data possession at untrusted stores,"Proc. ACM Conf. Comput. and Commun. Secur., pp. 598-610., 2007

[2] G. Ateniese, S. Kamara and J. Katz, "Proofs of storage from homomorphic identification

B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru and H. Rubens, "ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks", ACM Trans. Inform. Syst. Security, vol. 10, no. 4, pp. 1¿¿¿35, 2008

[4] Full Text: Access at ACM

B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru and H. Rubens, "ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks,"ACM Trans. Inf. Syst. Secur., vol. 10, no. 4, pp. 11-35, 2008

[5] Full Text: Access at ACM

K. Balakrishnan, J. Deng and P. K. Varshney, "TWOACK: Preventing selfishness in mobile ad hoc networks,"Proc.

IEEE Wireless Commun. Netw. Conf., pp. 2137-2142, 2005

[6] D. Boneh, B. Lynn and H. Shacham, "Short signatures from the weil pairing", J. Cryptol., vol. 17, no. 4, pp. 297-319, 2004 [CrossRef]

[7] S. Buchegger and J. Y. L. Boudec, "Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks),"Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Netw. Comput. Conf., pp. 226-236, 2002

[8] L. Buttyan and J. P. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks", ACM/Kluwer Mobile Netw. Appl., vol. 8, no. 5, pp. 579-592, 2003 [CrossRef]

[9] J. Crowcroft, R. Gibbens, F. Kelly and S. Ostring, "Modelling incentives for collaboration in mobile ad hoc networks", First Workshop Modeling Optimization Mobile, Ad Hoc Wireless Netw., 2003

[10] J. Eriksson, M. Faloutsos and S. Krishnamurthy, "Routing amid colluding attackers", Proc. IEEE¿¿ Int. Conf. Netw. Protocols,, pp. 184-193., 2007

[11] Abstract | Full Text: PDF (2882KB) | Full Text: HTML

W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic and W. Kellerer, "Castor: Scalable secure routing for ad hoc networks,"Proc. IEEE INFOCOM, pp. 1-9, 2010

[12] Abstract | Full Text: PDF (245KB) | Full Text: HTML

T. Hayajneh, P. Krishnamurthy, D. Tipper and T. Kim, "Detecting malicious packet dropping in the presence of collisions and channel errors in wireless ad hoc networks,"Proc. IEEE Int. Conf. Commun., pp. 1062-1067., 2009

[13] Abstract | Full Text: PDF (336KB) | Full Text: HTML

Q. He, D. Wu and P. Khosla, "Sori: A secure and objective reputation-based incentive scheme for ad hoc networks,"Proc. IEEE Wireless Commun. Netw. Conf., pp. 825-830., 2004

[14] D. B. Johnson, D. A. Maltz and J. Broch, Ad Hoc Networking, pp. 139-172., 2001, Addison-Wesley

[15] W. Kozma Jr. and L. Lazos, "Dealing with liars: Misbehavior identification via Renyi-Ulam games", Int. ICST Conf. Security Privacy in Commun. Networks, 2009. [CrossRef]

[16] W. Kozma Jr. and L. Lazos, "REAct: Resource-efficient accountability for node misbehavior in ad hoc networks based on random audits,"Proc. ACM Conf. Wireless Netw. Secur., pp. 103-110., 2009

[17] K. Liu, J. Deng, P. Varshney and K. Balakrishnan, "An acknowledgement-based approach for the detection of routing misbehavior in MANETs", IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536-550, 2006.

[18] Y. Liu and Y. R. Yang, "Reputation propagation and agreement in mobile ad-hoc networks,"Proc. IEEE WCNC Conf., pp. 1510-1515., 2003

Author's Profile

Mr.S.Ramana Reddy received M.Tech(CSE) Degree from School of Information Technology, Autonomous, and Affiliated to JNTUH, Hyderabad. He is currently working as Assistant Professor in the Department of Computer Science and Engineering in Nalgonda Institute of Technology and Science, Nalgonda, Telangana, India. His interests includes Object Oriented Programming, Operating System, Database Management System, Computer Networking, Cloud Computing and Software Quality Assurance.

S.Ramana Reddy
Email: ramana.yes@gmail.com
Phone no: 91+9848989364
Nalgonda Institute of Technology and Science
Cherlapally, Nalgonda-508001
Telangana.

Author's profile:

Mr. B. Mahender Reddy received M.Tech from JNTU and received B.Tech degree from JNTU. He is currently working as Assistant professor, Department of CSE, in Siddhartha Institute of Engineering & Technology, Ibrahimpatnam,RangaReddy District, Telangana, India. His interests include Wireless Sensor Networks, Operating Systems, C, C++ and JAVA.