International Journal of Engineering & Technology, 7 (1.2) (2018) 178-180

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Intelligent channel aware malicious free data forwarding scheme over wireless sensor networks

Mohammad Sirajuddin *

Assistance Professor Dept of CSE, Vaageswari College of Engineering Hyderabad -Karimnagar Highway,
Beside LMD Police Station, Ramakrishna Colony, Karimnagar, Telangana 505481
**Corresponding author E-mail: siraj569@gmail.com*

Abstract

In the communicative world each and every individual needs to perform global communication with failure-free intelligent model. Wireless Sensor Network, a medium which provides efficient communication modes to clients to satisfy their communication needs. However, this kind of wireless network channels are also facing lots of communication issues by means of several fault strategies, such as: link failures, node failures, bandwidth inefficiency, poor energy level, attacks and many more. So that, a fast growing network scheme is required as well as it provides lots of features to communication strategies and routing protocols, called Intelligent-Channel-Aware-Reputation Scheme [ICARS]. In the proposed system, the main objective is to provide the strong and failure-free wireless communication medium over networking with multiple numbers of nodes. As well as to provide high-level of security while the data is communicating from source to destination. For that powerful cryptographic algorithm is employed, called Modified Rijndael Algorithm (MRA) and to clearly state that the attack-free wireless communication channel with the help of intelligent routing strategies such as Route Request (RREQ) and Route Response (RREP).

Keywords: *Wireless Sensor Network; WSN; Intelligent-Channel-Aware-Reputation Scheme; ICARS; RREQ; RREP, Modified Rijndael Algorithm; MRA.*

1. Introduction

Wireless Sensor Networks [WSN], a leading communication norm, which provides several benefits to communicate with one entity to other entity without any interruptions. However, in terms of security and failures, we need to concentrate more into the WSNs to resolve those issues. So, that a new technology and some new protocols are required to resolve such issues. With this scheme the wireless channels can operate with more efficiency and performance, because of theses, routing protocols are highly-fault-tolerant to avoid the attacker nodes as well as provides the efficient communication between source and destination. The attacks in the network scenarios are: DOS, Wormhole attack and Blackhole attacks. In this system, a new routing protocol strategy is defined by means of Route Request and Route Response Strategies with the help of Intelligent-Channel-Aware-Reputation Scheme (ICARS) [1].

a) system analysis

Source Node sends Route Request to the nearby node. The nearby node checks the request and sends the Route Response to Source Node back within a proper interval. The proper and relevant response from the neighbor node indicates it as a proper node as well as the neighbor node sequence Number will get incremented by 1 [2]. The node is proper then only the count will be incremented otherwise it consists attack content. This kind of nodes are properly blocked from the present scenario and the source checks for the alternate or other neighbor nodes to proceed for further communications [3].

As per the regular network strategies the node selection or path selection process is purely based on Shortest Path Routing methodology. These kinds of activities are slightly changed and providing some good as well as efficient norms with the proposed routing logics to save time and financial needs. Instead of selecting the alternate route for the affected nodes, the idle nodes present into the wireless network near to the affected node is acting like an evaluator node as well as check the efficiency level of the affected node and provides the sufficient energy to the affected node to get back the affected node as a normal node and make it as eligible for further communications [4].

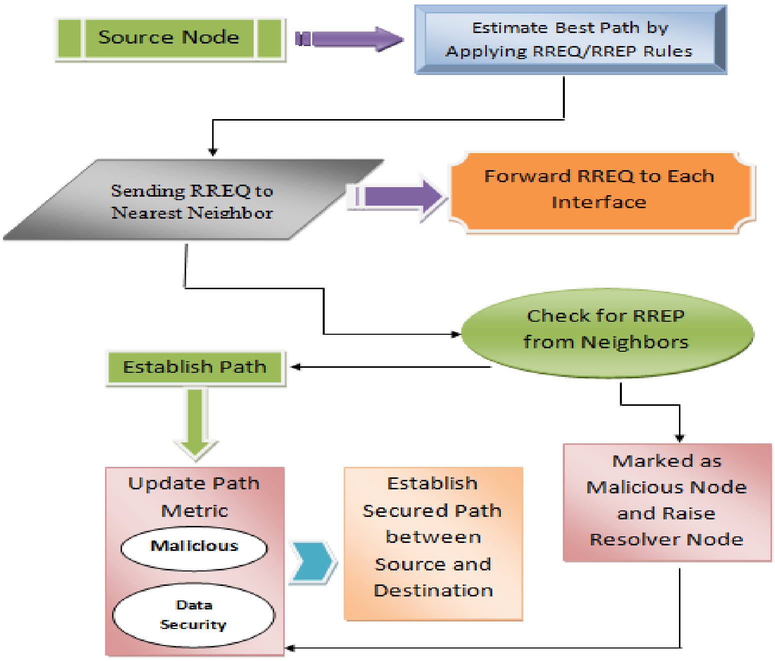
Source Node
Estimate Best Path by Applying RREQ/RREP Rules
Sending RREQ to Nearest Neighbor
Forward RREQ to Each Interface
Check for RREP from Neighbors
Establish Path
Update Path Metric
Malicious
Data Security
Establish Secured Path between Source and Destination
Marked as Malicious Node and Raise Resolver Node

Fig. 1: Proposed System Model.

So, that the node energy preserving is keep in a constant level and no nodes will be getting affected or else eliminated from the wireless network channel scenario. However, due to the insufficiency of physical protection over wireless sensor network, sensor nodes are easily compromised by adversaries, making wireless sensor network vulnerable to various security threats [5]. One of the most severe threats is selective forwarding attack, where the compromised nodes can maliciously drop a sub-set of forwarding packets to deteriorate the data delivery ratio of the network. It also has significantly negative impacts to data integrity, especially for data sensitive applications, for instance, health care and industry monitoring [6].

On the other hand, since WSNs are generally deployed in openareas' (for instance 'Primeval-Forest'), the unstable wireless channel requires more concentration and added security with the help of powerful cryptography algorithms, so that a new algorithm is introduced over here with enhanced security norms, called Modified Rijndael Algorithm (MRA), which takes care of data security with relevant features [7].

b) Attack-Free Intelligent Routing Scheme

The attackers are the major threats and issue in wireless sensor network as well as they affect the wireless node at major level with cracking techniques. So, that the wireless sensor network uses some intelligent routing schemes like AODV, DSR to prevent these issues [8]. However, these kind of reverting mechanisms are time consumed and cost enhancement process. So that in the proposed approach a new logic is devised, such as forming the Evaluator/Resolver Node at dynamic instant, Which identifies the affected node by checking the computational power of the node, means which node having low computational power that will not be able to respond properly for the data routing request from neighbors, in that case it will be marked as a attacked/malicious/fault node [9].

In this case Evaluator/Resolver Node is generated dynamically by the network routing scenario and that node acts as a Resolver node to resolve this issues caused by passing a supplement power to the affected node. The proposed approach focuses on attack free wireless communication medium with the help of Modified AODV Protocol [10].

c) Proposed Approach – A Summary

The proposed protocol determines two main functionalities:

- Route Discovery and
- Route Maintenance

In proposed approach Source Node sends Route REQuest (RREQ) to nearby node. The nearby node checks it and forward Route REPly (RREP) to Source Node. If so the neighbor node is a proper node. In neighbor node sequence Number will incremented by 1 count [11]. If the node is proper then only the count will be incremented otherwise it consist attack. Selecting Neighbors based on Shortest Path, so the performance is good as well. In the traditional approaches all the communications and their channel definitions are static. Because before start defining the number of nodes in network bandwidth efficiency, transmission speed, reception speed and their pathway are manipulated and based on that only route will be established. This is not suitable for the case when the transmission range will grow or else shorten, in the similar manner if the number of node increases the entire network flow will getting decreases and it is not suitable for dynamic scenarios [12].

We propose a new approach to eliminate one or multiple black hole nodes on AODV routing protocol. In our approach, the intermediate node forwards the valid route reply to the next node. The invalid routes replies are avoided by intermediate nodes in the overall network. Attack possibilities are highly preserved with the help of advanced routing protocols such as AODV, as well as the protocol nature is highly modified with the parameters such as reception power and transmission power [13]. For all with the help of Route Request and Route Response Schemes we can prove our proposed approach is more efficient and suitable for scalable environment.

2. Literature survey

In the year of 2015, the authors "J. Ren, Y. Zhang, K. Zhang, and X. Shen" proposed a paper titled "Sacrm: Social aware crowdsourcing with reputation management in mobile sensing", in that they described such as: Portable detecting has turned into a promising worldview for versatile clients to get data by errand crowdsourcing. In any case, because of the social inclinations of portable clients, the nature of detecting reports might be affected by the basic social traits and childishness of people. Consequently, it is significant to consider the social effects and reliability of portable clients while choosing errand members in versatile detecting [8], [13].

In this paper, we propose a Social Aware Crowdsourcing with Reputation Management plan to choose the appropriate members and apportion the undertaking rewards in versatile detecting. In particular, we consider the social traits, errand postponement and notoriety in crowdsourcing and propose a member choice plan to pick the appropriate members for the detecting undertaking under a settled assignment spending plan. A report evaluation and compensating plan is likewise acquainted with measure the nature of the detecting reports and distribute the assignment rewards based the surveyed report quality. Likewise, we build up a notoriety administration plan to assess the reliability and cost execution proportion of versatile clients for member determination. Hypothetical examination and broad reproductions exhibit that SACRM can proficiently enhance the crowdsourcing utility and successfully invigorate the members to enhance the nature of their detecting reports.

In the year of 2013, the authors "E. Shakshuki, N. Kang, and T. Sheltami" proposed a paper titled "Eaacka secure intrusion detection system for manets", in that they described such as: the movement to remote system from wired system has been a worldwide pattern in the previous couple of decades. The portability and versatility brought by remote system made it conceivable in numerous applications. Among all the contemporary remote systems, Mobile Ad hoc NETwork (MANET) is a standout amongst the most imperative and one of kind applications [14].

On the in opposition to conventional system design, MANET does not require a settled system framework; each and every hub acts as both a transmitter and a collector. Hubs discuss straightforwardly with each other when they are both inside a similar correspondence go. Else, they depend on their neighbors to transfer messages. The self-designing capacity of hubs in MANET made it prominent among basic mission applications like military utilize or crisis recuperation. Nonetheless, the open medium and wide dispersion of hubs make MANET powerless against noxious aggressors. For this situation, it is critical to create proficient interruption discovery systems to shield MANET from assaults. With the changes of the innovation and cut in equipment costs, we are seeing a present pattern of growing MANETs into mechanical applications. To change in accordance with such pattern, we emphatically trust that it is crucial to address its potential security issues. In this paper, we propose and actualize another interruption location framework named Enhanced Adaptive ACKnowledgment (EAACK) uncommonly intended for MANETs. Contrasted with contemporary methodologies, EAACK exhibits higher pernicious conduct location rates in specific conditions while does not extraordinarily influence the system exhibitions.

3. Conclusion

In this proposed system, channel aware-and-failure free routing scheme is introduced with more intelligent factors and powerful algorithms. Through the advantages of proposed algorithms called Intelligent-Channel-Aware-Reputation Scheme [ICARS] and Modified Rijndael Algorithm [MRA], we can assure the data to be reached into the destination properly without any failures and attacks. The proposed techniques such as Evaluator/Resolver Node Generation and Route Request and Response techniques are an added advantage to the proposed wireless sensor network model. With the help of the proposed system, the wireless network maximization strategies such as throughput, delay, lifetime and Packet Delivery Ratio (PDR) are getting improved and the experimental results will show the proof for that in fine manner.

References

[1] I. Butun, S. Morgera, and R. Sankar, “A survey of intrusion detection systems in wireless sensor networks,” IEEE Commun. Surv. & Tutor. vol. 16, no. 1, pp. 266–282, 2014. https://doi.org/10.1109/SURV.2013.050113.00191.

[2] Y. Zou, X. Wang, and W. Shen, “Physical-layer security with multiuser scheduling in cognitive radio networks,” IEEE Trans. Commun., vol. 61, no. 12, pp. 5103–5113, 2013. https://doi.org/10.1109/TCOMM.2013.111213.130235.

[3] B. Xiao, B. Yu, and C. Gao, “Chemas: Identify suspect nodes in selective forwarding attacks,” J. Parallel Distributed Comput., vol. 67, no. 11, pp. 1218–1230, 2007. https://doi.org/10.1016/j.jpdc.2007.04.014.

[4] Y. Zhang, L. Lazos, and W. Kozma, “Amd: Audit-based misbehavior detection in wireless ad hoc networks,” IEEE Trans. Mob. Comput., prePrints, published online in Sept. 2013.

[5] S. Ozdemir, “Functional reputation based reliable data aggregation and transmission for wireless sensor networks,” Comput. Commun, vol. 31, no. 17, pp. 3941–3953, 2008. https://doi.org/10.1016/j.comcom.2008.07.017.

[6] D. Hao, X. Liao, A. Adhikari, K. Sakurai, and M. Yokoo, “A repeated game approach for analyzing the collusion on selective forwarding in multihop wireless networks,” Comput. Commun, vol. 35, no. 17, pp. 2125–2137, 2012. https://doi.org/10.1016/j.comcom.2012.07.006.

[7] X. Liang, X. Lin, and X. Shen, “Enabling trustworthy service evaluation in service-oriented mobile social networks,” IEEE Trans. Parallel Distr. Sys., vol. 25, no. 2, pp. 310–320, 2014. https://doi.org/10.1109/TPDS.2013.37.

[8] J. Ren, Y. Zhang, K. Zhang, and X. Shen, “Sacrm: Social aware crowdsourcing with reputation management in mobile sensing,” Computer Commun., vol. 65, no. 15, pp. 55–65, 2015. https://doi.org/10.1016/j.comcom.2015.01.022.

[9] L. Yu, S. Wang, K. Lai, and Y. Nakamori, “Time series forecasting with multiple candidate models: selecting or combining,” J. Sys. Sci. Complexity, vol. 18, no. 1, pp. 1–18, 2005.

[10] J. Ren, Y. Zhang, K. Zhang, and X. Shen, “Exploiting channel-aware reputation system against selective forwarding attacks in wsns,” in Proc. IEEE GLOBECOM, 2014, pp. 330–335. https://doi.org/10.1109/GLOCOM.2014.7036829.

[11] S. Djahel, F. Nait-Abdesselam, and Z. Zhang, “Mitigating packet dropping problem in mobile ad hoc networks: proposals and challenges,” IEEE Commun. Surv. & Tutor. vol. 13, no. 4, pp. 658–672, 2011. https://doi.org/10.1109/SURV.2011.072210.00026.

[12] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan, “An acknowledgment-based approach for the detection of routing misbehavior in manets,” IEEE Trans. Mob. Comput, vol. 6, no. 5, pp. 536–550, 2007. https://doi.org/10.1109/TMC.2007.1036.

[13] E. Mahmoud and X. Shen, “An integrated stimulation and punishment mechanism for thwarting packet dropping attack in multihop wireless networks,” IEEE Trans. Vehic. Tech., vol. 60, no. 8, pp. 3947–3962, 2011. https://doi.org/10.1109/TVT.2011.2162972.

[14] E. Shakshuki, N. Kang, and T. Sheltami, “Eaacka secure intrusiondetection system for manets,” IEEE Trans. Ind. Electro., vol. 60, no. 3, pp. 1089–1098, 2013. https://doi.org/10.1109/TIE.2012.2196010.

[15] T. Shu and M. Krunz, “Detection of malicious packet dropping in wireless ad hoc networks based on privacy-preserving public auditing,” in Proc. ACM WiSec, 2012, pp. 87–98. https://doi.org/10.1145/2185448.2185460.

[16] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in Proc. ACM MobiCom, 2000, pp. 255–265. https://doi.org/10.1145/345910.345955.

[17] X. Li, R. Lu, X. Liang, and X. Shen, “Side channel monitoring: packet drop attack detection in wireless ad hoc networks,” in Proc. IEEE ICC, 2011, pp. 1–5.

[18] T. Shu, M. Krunz, and S. Liu, “Secure data collection in wireless sensor networks using randomized dispersive routes,” IEEE Trans. Mob. Comput, vol. 9, no. 7, pp. 941–954, 2010. https://doi.org/10.1109/TMC.2010.36.

[19] A. Liu, Z. Zheng, C. Zhang, Z. Chen, and X. Shen, “Secure and energyefficient disjoint multipath routing for wsns,” IEEE Trans. Vehic. Tech., vol. 61, no. 7, pp. 3255–3265, 2012. https://doi.org/10.1109/TVT.2012.2205284.

[20] S. Li, S. Zhao, X. Wang, K. Zhang, and L. Li, “Adaptive and secure load-balancing routing protocol for service-oriented wireless sensor networks,” IEEE Sys. Journal, vol. 8, no. 3, pp. 858–867, 2014. https://doi.org/10.1109/JSYST.2013.2260626.