ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Energetic Network Throughput Optimization and Attack Prevention 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, India

ABSTRACT: In Wireless Sensor Networks, more concentration is required for security and communication as well as node energy prevention. Various kinds of protocols are used to enhance the network lifetime and security. Security oriented algorithms which is implemented earlier is totally insecure in the case of Denial-of-Service [DoS] attacks. Usually Denial-of-Service attacks reduce the energy of the nodes presented into the respective network and track the data from those nodes. In order to eliminate these kinds of problems a new protocol is introduced additionally with Machine Access Code [MAC], called Modified Adhoc-On-Demand-Distance-Vector [MAODV], which counters the replay attack and forge attack in an energy-efficient way. The entire implementation of the proposed system concentrates highly on data security along with Wireless Sensor Network communications. With the help of this system, user can feel relax while entering into communication environments and perform failure-free data communications between source and destination entities with full of security. For all the proposed system experimentally proves the concept of data security with intelligent data transmissions from source to destination as well as increasing the throughput and lifetime of the Wireless Sensor Network.

KEYWORDS: Throughput, Denial-of-Service, DoS, Modified Adhoc-On-Demand-Distance-Vector, MAODV, Wireless Sensor Network.

I.INTRODUCTION

Wireless Sensor Networks are the recent trend in the communication domain, all the data transmission now-a-days is performed via wire-free communication medium with intelligent channel accessing facilities. A WSN is considered as a powerful-communication medium and it is highly utilized in secure domains such as military'-environments and civil-environments. However', some of the attacking norms such as Denial-of-Service [DOS] and so on, will disturb the wireless medium and affects the data transmission between source and destination. The normal data transmission protocols such as AODV, DSR and so on are all used to prevent the network with ultimate norms, but over that efficiency some intelligent norms are required to improve the efficiency of the wireless sensor networks.

An enhanced AODV, called Modified Adhoc-On-Demand-Distance-Vector (MAODV) is introduced into the proposed approach to attain the security and communication needs in finer manner. This leads to the entire network to enhance its throughput level and lifetime increase.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

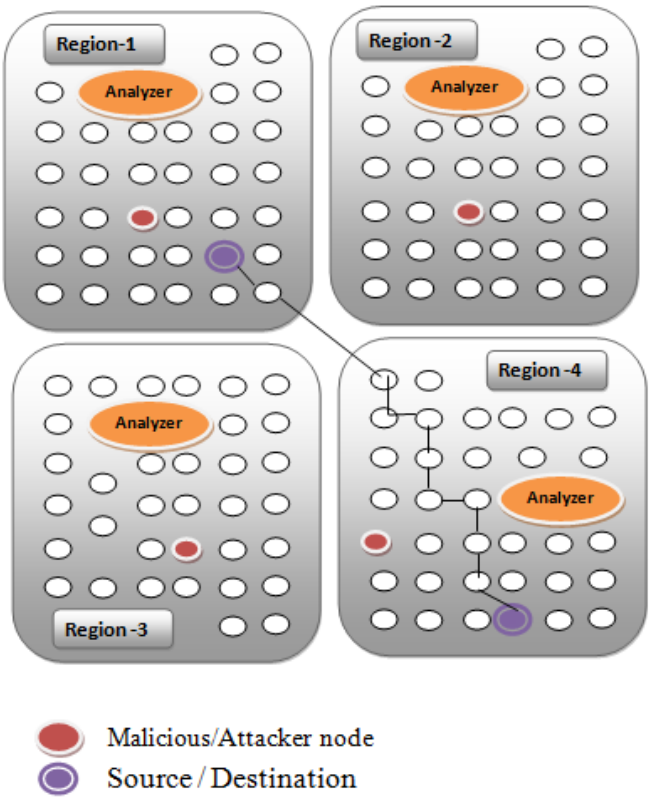

Fig.1 System Replication

A. Proposed System Summary

In the proposed approach, we introduce a new protocol called Modified Adhoc-On-Demand-Distance-Vector [MAODV] to enhance the lifetime and throughput of the wireless sensor network by reducing the security threats like DoS and improve the proficiency of data communications. We have to create a Wireless Network Architecture with n number of wireless nodes. Sender Node is formed automatically and it has to find out the nearest neighbor to transmit the packets from source to destination, once the neighbor node is selected the source doesn't form the path directly to transmit the data, instead of that it sends the route request to identify the localization and the neighbor node's ability to receive the packet. Once the Neighbor Node response to the particular route request then only source fix that node as a next successful neighbor and establish the path between them, otherwise mark that node as malicious in blacklist or routing table. Once the Malicious node is identified and blocked the source search for next nearest neighbor to find out the path to transfer packets. For enhancing the security constraints over transmission we add cryptographic algorithm to encrypt the data and pass it to receiver, once the receiver receives the data and then it has to be decrypted automatically.

B. Attack-Elimination Strategies

In traditional wireless security mechanisms, the transmitting data is encrypted with keyed symmetric or asymmetric encryption algorithm. The wireless sensor networks prefer the symmetric algorithm to avoid the complicated computing and heavy energy consumption. But the encrypted data makes the battery exhaustion even worse under Denial-of-Service attack. The attacker-node can send the encrypted "un-wanted" data to receiver. This attack forces the receiver to decrypt the data. Before the receiver identifies that the data is "un-wanted", the receiver consumes more power to receive and decrypt data. These processes also keep sensor nodes awake longer. An easy and fast mutual authentication scheme is needed to integrate with Machine Access Code protocol to counter the encrypted "un-wanted" data attack. This system proposes a two tier secure transmission scheme. This scheme uses the hash chain

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

to generate the dynamic session key, which can be used for mutual authentication and the symmetric encryption key. The only computations of dynamic session key are the hash functions, such as MD5 or SHA1, which are very simple and fast. By integrating with MAC protocol, there is no extra packet compared with the existing MAC designs. The security analysis shows that this scheme can counter the replay attack and forge attack, and the energy analysis shows that this scheme is energy efficient as well.

II.LITERATURE SURVEY

In the year of 2013, the authors "E. Shakshuki, N. Kang, and T. Sheltami" proposed a paper titled "Eaacka secure intrusiondetection 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 versatility and adaptability 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 essential and extraordinary applications. On the in opposition to customary system design, MANET does not require a settled system framework; each and every hub fills in as both a transmitter and a beneficiary. Hubs discuss straightforwardly with each other when they are both inside a similar correspondence go. Else, they depend on their neighbors to hand-off messages. The self-designing capacity of hubs in MANET made it prominent among basic mission applications like military utilize or crisis recuperation. In any case, the open medium and wide dissemination of hubs make MANET defenseless against pernicious aggressors. For this situation, it is vital to create effective interruption recognition systems to shield MANET from assaults. With the upgrades of the innovation and cut in equipment costs, we are seeing a present pattern of growing MANETs into mechanical applications. To acclimate to such pattern, we firmly trust that it is imperative to address its potential security issues. In this paper, we propose and actualize another interruption recognition framework named Enhanced Adaptive ACKnowledgment (EAACK) uniquely intended for MANETs. Contrasted with contemporary methodologies, EAACK shows higher pernicious conduct identification rates in specific conditions while does not extraordinarily influence the system exhibitions.

In the year of 2012, the authors "K. Govindan and P. Mohapatra" proposed a paper titled "Trust computations and trust dynamics in mobile adhoc networks: a survey", in that they described such as: trust is a critical part of versatile adhoc systems (MANETs). It empowers elements to adapt to vulnerability and wildness caused by the choice of others. Trust calculations and administration are exceptionally testing issues in MANETs because of computational multifaceted nature imperatives, and the free development of part hubs. This keeps the immediate use of systems suited for different systems. In MANETs, a dishonest hub can wreak extensive harm and unfavorably influence the quality and unwavering quality of information. Accordingly, investigating the trust level of a hub impacts the certainty with which an element conducts exchanges with that hub. In this work we show a nitty gritty overview on different trust processing approaches that are outfitted towards MANETs. We feature the outline and examinations of these methodologies. Furthermore, we dissect different chips away at trust flow including confide in proliferation, expectation and accumulation calculations, the impact of system elements on trust progression and the effect of trust on security administrations.

III.CONCLUSION

In the proposed approach, the failure-free communication model is designed for Wireless Sensor Networks data transmission scheme. This system introduces a new methodology/protocol called Modified AdHoc Distance Vector Routing [MAODV], which eliminates the attacks caused by Denial-of-Service [Dos] as well as improve the data security by means of enhancing the throughput and lifetime of the wireless sensor network. For all the entire system is more useful to perform wire-free communications and provide full support to users to perform data transmissions with threat free mechanism.

REFERENCES

[1] G. P. Halkes, T. V. Dam, and K. Langendoen, “Comparing energysaving mac protocols for wireless sensor networks,” ACM Mobile Networks and Applications, vol. 10, no. 5, pp. 783-791, Oct. 2005.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

[2] A. Bachir, M. Dohler, T. Watteyne, and K.K. Leung, "MAC essentials for wireless sensor networks," IEEE Communications Surveys & Tutorials, vol.12, no.2, pp. 222-248, Second Quarter 2010.
[3] W. Ye, J. Heidemann, and D. Estrin, "An energy-efficient mac protocol for wireless sensor networks," in Proc. INFOCOM, New York, 2002, pp. 1567- 1576.
[4] T. van Dam and K. Langendoen, "An adaptive energy-efficient mac protocol for wireless sensor networks," in Proc. ACM SenSys, Los Angeles, 2003, pp. 171-180.
[5] J. Polastre, J. Hill, and D. Culler, "Versatile low power media access for wireless sensor networks," in Proc. ACM SenSys, Baltimore, 2004, pp. 95-107.
[6] M. Buettner, G. V. Yee, E. Anderson and R. Han, "X-MAC: a short preamble MAC protocol for duty-cycled wireless sensor networks," in Proc. ACM SenSys, Boulder, 2006, pp. 307-320.
[7] M. Brownfield, Y. Gupta, and N. Davis, "Wireless sensor network denial of sleep attack," in Proc. 6th Annu. IEEE SMCIAW, 2005, pp. 356-364.
[8] D. Raymond, R. Marchany, M. Brownfield and S. Midkiff, "Effects of denial of sleep attacks on wireless sensor network MAC protocols," IEEE Transactions on Vehicular Technology, vol. 58, no. 1, Jan. 2009.
[9] R. Falk, and H.J. Hof, "Fighting insomnia: a secure wake-up scheme for wireless sensor networks," in Proc. SECURWARE, Athens, 2009, pp. 191-196.
[10] Y. C. Ouyang, R. L. Chang, and J. H. Chiu, "A new security key exchange channel for 802.11 WLANs," in Proc. IEEE ICCST, Taipei, 2003, pp. 216-221.
[11] Y. C. Ouyang, C. B. Jang, and H. T. Chen, "A secure authentication policy for UMTS and WLAN interworking," in Proc. IEEE ICC, Glasgow, 2007, pp. 1552-1557.
[12] Y. C. Ouyang, C. T. Hsueh, and H. W. Chen, "Secure authentication policy with evidential signature scheme for WLAN," Security and Communication Networks, vol. 2, no. 3, May/June 2009, pp. 259-270.
[13] N. Haller, and C. Metz, "A one-time password system," IETF RFC 2289, Feb. 1998.
[14] D. W. Carman, P. S. Kruus, and B. J. Matt, "Constraints and approaches for distributed sensor network security," NAI Labs, The Security Research Division, Glenwood, Tech. Rep. #00-010, Sept. 2000.
[15] P.Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu, "Analyzing and modeling encryption overhead for sensor network nodes," in Proc. ACM WSNA, San Diego, 2003, pp. 151-159.
[16] W. Liu, R. Luo, and H. Yang, "Cryptography overhead evaluation and analysis for wireless sensor networks," in Proc. WRI CMC, Kunming, 2009, pp.496-501.
[17] C. T. Hsueh, Y. W. Li, C. Y. Wen, and Y. C. Ouyang, "Secure adaptive topology control for wireless ad-hoc sensor networks," Sensors, vol. 10, no. 2, 2010, pp. 1251-1278.
[18] K. T. Chu, C. Y. Wen, Y. C. Ouyang, and W. A. Sethares, "Adaptive distributed topology control for wireless ad-hoc sensor networks," in Proc. SensorComm, Valencia, 2007, pp. 378-386.
[19] Crossbow MicaZ datasheet, Crossbow Technology Inc., 2006.
[20] Atmel ATmega 128L datasheet, Atmel Corporation, 2009.

BIOGRAPHY

MOHAMMAD SIRAJUDDIN has currently working as an Assistant Professor in CSE department, Vaageswari college of engineering, Beside LMD Police station, Hyderabad - Karimnagar Highway Ramakrishna Colony, Karimnagar, Telangana. He completed B.Tech in Mother Theresa Institute of technology and science in 2006 and M.Tech in Royal Institute of tech and science in 2011. His research interest areas in Wireless sensor networks, he has 5yrs experience in teaching.