ISSN 1512-1232

Securing Wireless Sensor's Network Using Mobile Ad-hoc On Demand Data Delivery Protocol (MAODDP)

Humayun Bakht

Research Fellow, London School of Commerce, United Kingdom
humayunbakht@yahoo.co.uk

Abstract

Wireless Sensor's networks (WSN's) are type of wireless ad hoc networks with reduced or no mobility. These networks combine wireless communication with minimal onboard computation facilities for sensing and monitoring of environment. Much work has been reported on different aspects of wireless sensor's networks; however, less attention has been paid on addressing secure communications in these networks. It is due to the nature of these networks; an intruder can access or interrupt an ongoing communication session. Therefore, security attains prime importance thus require a solution which can address specific requirements and can be deployed at ease. Moreover, the propose solution should be able to expand it self without any additional burden to the resources should the network grow. Mobile Ad-hoc On Demand Data Delivery Protocol (MAODDP) belongs to on-demand data delivery type routing family of mobile ad-hoc networks. MAODDP has been extended to offer similar services in WSN's. The contribution of this paper is to introduce an efficient security mechanism for securing communication over WSN's network. We believe the proposed solution can be deployed with minimal consumption of the limited resources.

Keywords: *Mobile Ad-hoc On Demand Data Delivery Protocol (MAODDP); Wireless Sensor's Networks (WSN's); Mobile Ad-hoc Network (MANET); Authentication WSN's; Secure WSN's*

1. Introduction

With the recent advances in technologies miniaturization of computing and sensing technologies enables the development of tiny, and low-cost sensors and controller [1]. There is an increasing focus on these systems is observed in the civil domain to monitor and to protect critical infrastructure such as bridges and tunnels etc. [2]. Such wireless networks of distributed sensor nodes are commonly known as Wireless Sensor Networks (WSNs) [3]. WSN's have its origin from mobile ad-hoc network [4]. Mobile ad-hoc network (MANET) is the collection of mobile nodes establishing network without any supporting infrastructure [5]. A WSN's suffers many of the same issues as a MANET. Some of these issues are security and battery power. Sensors link the physical world with the digital world by capturing, interacting and revealing real-world objects into a form that can be stored, processed and analyzed [6]. Sensor can help to monitor and avoid catastrophic infrastructure failures, conserve precious natural resources, increase productivity, and enable new applications such as smart homes and smart cities technologies [7-8]. Mobile ad-hoc on-demand data delivery protocol (MAODDP) is an on-demand data delivery protocol focusing route establishment and data delivery one after the other simultaneously at the same time [9]. They key feature of MAODDP is the integral approach which allows protocol to address routing alongside other interrelated issue. MAODDP has been extended to support similar operation in related network and has been successful in addressing fault discovery and management in WSN's. The contribution of this work is to introduce a novel security mechanism for WSN's. In this context, this work has been organized as follows. In section 2 A detail overview of the proposed secure

ISSN 1512-1232

mechanism is presented. In section 3 a conclusive discussions highlighting benefits of the proposed scheme is presented and conclusion and future work is covered in section 4.

2. Secure Mechanism for Wireless Sensor's Network

In MAODDP, a wireless sensors network formation follows clusters structure which is further divided into main controller and sub controllers. In this context, registration phase is divided into external registration and internal registration. Nodes having highest computational and battery power are selected to be cluster heads for all the potential clusters. A node having the shortest distance with the base station or where the collected data is transferred is selected as the main controller. The same principle applied when selecting the chain of clusters. In due course main controller registers all the clusters as sub controllers who in turns register nodes as their respective group members. The novelty of the security mechanism lies in the fact that the adopted security principles are applicable from top to bottom network formation. In other words, any new network which could be established within a cluster can follow the same strategy to acquire secure communication. The following operations are defined by the MAODDP secure mechanism.

2.1. Broadcasting Controller Request

This request is broadcasted by the sensors networking having high computational power to the base station or main collection point. The selection of main controller is based on the two factors namely shortest distance to the base station and highest computational power. Once the selection of main controller is made sub controllers are assigned using the same principle outline above. In other words, the node having the second shortest distance is assigned as sub controller one, the one having the second shortest distance to the base station is assigned as sub controller two and vice versa. This list is then broadcasted for all other nodes to update about the potential list of sub controllers to join during the formation of the network.

It is important to note that both main controller and sub controller are assigned a UNIQUE VERIFICATION KEY (UVK) during the selection and authentication phase. This key is recorded and stored at an allocated table at the base station. This eliminates the chances for an intruder to interrupt any communication especially when collected data is transmitted from the sub controller to the main controller. It is important to note that in order to establish a trust relation between the controller and main controller a separate message is send to each of the controllers to inform them assigned UVK of the participating controllers. This message is secured using the same keys and is distained only for the selected controllers.

2.2. External Registration

Each of the sub controllers registered first with the main controller through external registration request. Main controller in return sends a registration confirmation with a unique key added to the UVK to the sub controller who initiated external registration process. It is important to state that all the data which is send to main controller is in encrypted form and cannot be decrypted by the intermediate sub controllers forming route to the main controller. Main controller can verify any sender through the combination of UVK and the unique key which was allocated to individual sub controllers during the external registration phase.

2.3. Network Formation and Internal Registration

Each of the sub controllers broadcast a Joining invitation to the neighboring or nodes in its range. Nodes on receiving joining invitation if wants to be part of network send back the accept notification to the sub controller through the same path it receive joining invitation. Sub controller

ISSN 1512-1232

on receiving accepted notification sends an encrypted key with a randomly generated sequence number back to the nodes. This information is also stored within sub controllers in order to identifying nodes as legitimate in any future communication. Once the internal registration process is completed a list with the member's nodes is issued which is destined to registration nodes only. This list contains nodes sequence number and the two decrypted letters of the three letters encrypted key assigned to individual nodes at the internal registration process. Each of the participating nodes stores this information to identify other nodes in any future communication. It is important to mention that the third letter of the three digits key of individual node can only be encrypted at sub controller.

3. Discussion

MAODDP introduced a novel mechanism to secure wireless sensor's network. This work can be seen as an extention of the previous reported work addressing fault discovery and management. The key feature of the above mentioned scheme is providing security both at the time of network formation and during inter and intra communication. In addition, purposed scheme addresses concerned issue with some exisiting problems including limited power and available bandwidth. MAODDP also reduces control packets numbers thus reducing any further burden on network thereby minimizing possiblities of network congestion which can lead a potential security hole in a WSN. Moreover, another benefit of MAODDP secure mechanism is ensuring nodes are available for actual data collection and transmission.

4. Conclusion and Future Work

The contribution of this work is to present novel security architecture for Wireless Sensor's Network. MAODDP was initially developed to provide communication support for a mobile ad-hoc network. It has been successfully extended to provide various functionalties for related network. MAODDP secure mechanism for WSN's not only provide a unique method of providing security but also adopts a novel stratgey of network formation and delopment. In future, we will be combining related work in parts in order to offer a more enhanced form of fault discovery and management and secure communication architecture for WSN's. We are committed to contribute our findings with the ongoing research in this area.

ISSN 1512-1232

5. References

1. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, A survey on sensor networks," presented at the IEEE Communication Magazine, 2002.
2. H. Karl and A. Willig, Protocols and Architectures for Wireless Sensor Networks: John Wiley & Sons, Ltd, West Sussex, England, 2005.
3. B. krishnamachari, Networking Wireless Sensors: Cambridge University Press, New York, 2005.
4. K. Sohraby, D. Minoli, and T. Znati, Wireless Sensor Networks: Technology, Protocols, and Applications. Hoboken, New Jersey: John Wiley & Sons, Inc, 2007.
5. H.Bakht, Mobile Ad-hoc Networking, Create Space, January 2010.
6. I. F.Akyildiz and M. C. Vuran, Wireless Sensor Networks. A John Wiley and Sons, Ltd, Publication, August 2010.
7. C. Cordeiro and D. P. Agrawal, Ad hoc & sensor networks, Theory and Applications: World scientific publishing, 2006.
8. S. Gupta and N. Parveen, "Optimum Node Deployment Strategy for Heterogeneous Wireless Sensor Network by Estimating Network Lifetime," presented at the 2nd International Conference on Emerging Trends in Engineering and Technology (ICETET'09), 2009.
9. HBakht, “Short Live Networking”, CreateSpace, Novmber 2014.

Article received: 2015-08-28