RESEARCH ARTICLE OPEN ACCESS

Improving the Quality of Services in Wireless Sensor Network by Improving the Security

Mr. Ajay Ramesh Karare[1], Prof.S.V.Sonekar[2], Miss. Kumari Akanksha[3]
Post Graduate Department of CSE, JDCOEM, RTMNU, Nagpur India
Email: ajju.karare@gmail.com[1], srikantsonekar@rediffmail.com[2]
Department of CSE Jhulelal Institute of Technology, RTMNU, Nagpur India
Email:, kumariakanksha5@gmail.com[3]

ABSTRACT
Wireless Sensor Network (WSN) is been used very widely over the recent years in the various field such as Defence, medical research, Security and many more, because of its advantages such as WSN can pass through any physical partition, it can accommodate any new node at any time. Wireless sensor networks include spatially allotted autonomous instruments that employ sensors to check environmental or physical conditions. These autonomous instruments, or nodes, blend with routers and an entrance to make a standard WSN system. The allotted measurement nodes wirelessly communicate to a central entrance that gives a connection to the wired world in which users can gather, process, examine and present their evaluated data. However for the WSN designer the biggest issue is to fulfill the Quality of Services (QoS) imposed by the application (& user). Quality of service (QoS) concepts has not been applied to wireless sensor networks (WSNs) until recently. QoS support is challenging due to severe energy and computational resource constrains and the security of wireless sensors In this paper we have discussed the security parameter for degrading the QoS in the WSN and also the corrective measures to improve the QoS by improving the security in WSN by using SAFEQ and extended watchdog algorithm

Keywords – Wireless Sensor Network, Security, Quality of Service, SAFEQ, Watchdog .

I. Introduction

Wireless Sensor Networks (WSNs) are envisioned to be the next generation of networks which will form an integral part of man's lives. The sensor nodes are usually small in size, with multi-modal sensing capabilities which allows them to collect raw data of various physical parameters such as temperature, salinity, humidity, light intensity, pressure, sound, radiation, etc. They are equipped with wireless interfaces, enabling them to communicate with each other via multiple hops using Radio Frequency (RF) techniques. Due to the miniature size of these nodes, sensor networks can be densely deployed in a distributed manner in any terrain; therefore the nodes need to have self-organizing and self-configuring capabilities, as like in ad hoc networks. With advances in wireless communications, the applications of sensor networks are no longer limited to that of periodic monitoring of the environment. Wireless sensor networks can be used for a wide array of applications spanning multiple domains – healthcare, biometrics, home networking, military, automotive, as well as construction and manufacturing industries. The sensor nodes typically obtain raw data from the environment in which they are deployed, and then send the collected information back to a centralized sink (or repository) where more complex processing and real-time analysis can be performed on the data.[1]

Hence, sensor networks can now be used for the following purposes:
(i) Data Acquisition – the collection of data from the environment;
(ii) Data Dissemination – the delivery of information to other nodes in the network;
(iii) Data Distribution – the delivery of information or instructions from the centralized sink to one or more sensor nodes in the network; and
(iv) M2M (Machine-to-Machine) communication – the provision of a platform for interactions between machines and the environment, without unnecessary terminal will get reduced.

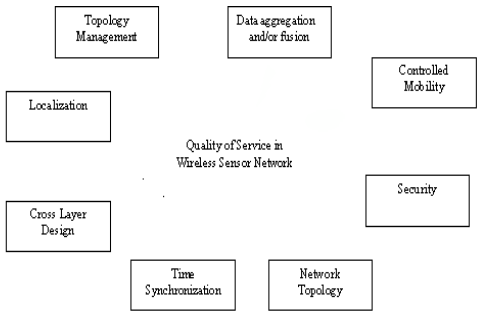

Fig. 1: WISER – a framework to achieve QoS in Wireless Sensor networks

There are different parameters for measuring the quality of services in Wireless Sensor Network as shown in above Fig as Topology Management, Data Aggregation and/ or fusion, Controlled mobility, Localization, Cross Layer design Time Synchronization, Network topology and Security. Out of above all parameters, in this paper we will be focusing on the parameter security for improving the Quality of Services in Wireless Sensor Network by using SAFEQ and watchdog algorithm.[2]

Security: The openness of the physical environment and the transmission media subjects sensor networks to a multitude of security attacks ranging from Denial of Service (DoS) to malicious attempts to modify sensitive data information. Consequently, it is quintessential to ensure that sensor networks incorporate security mechanisms into their protocols to protect the integrity of the data collected.

II. Related Work And Motivation

A. Existing QoS Mechanisms

The existing QoS mechanisms can be classified into two main categories:

i. Resource reservation; and
ii. traffic classification.

In resource reservation, network resources such as bandwidth are allocated according to the QoS requirements of the application. This necessitates the presence of a signalling or handshaking protocol such as RSVP, to reserve the required resources in each node along the path of the data packet, before the application is actually allowed to run. In addition, a call admission control protocol such as that proposed by Iraqi and Boutaba in – which regulates the permissible number of connections that can be allowed into the system while still fulfilling the QoS requirements of the application – is required.[4]

Traffic classification involves the categorization of data packets into different levels of priority, or classes of service (CoS), based on the application requirements. These data packets are marked with their respective classes at the edge of the network, and preferential treatment is then given to the traffic classes with higher priority as they pass through each hop along the path.[8] Traffic prioritization can be in the form of congestion management schemes such as scheduling, congestion avoidance or rate limiting. In general, data packets with lower priority are usually dropped at a higher rate than those with higher priority; this allows data flows with higher priority to have better QoS performance metrics such as reliability, end-to-end delay and throughput.

B. QoS Provisioning in WSNs

Wireless sensor networks have been envisioned for a wide range of applications, some of which may involve the collection of sensitive or critical data. For example, if underwater sensor nodes are thrown into the sea to monitor seismic activities and forewarn the possible occurrence of an earthquake or tsunami, the sensor network is not very useful if it is unable to inform the sink in time, on the impending natural disaster. Although delay is not a very crucial factor in sensor network applications such as periodic monitoring, shorter delays will nevertheless, be much desired over higher delays. Future WSNs may also be able to capture videos or snapshots of the physical environment and transmit these images (or videos) back to the sink for real-time data analysis. As such, there is a demand for QoS support in WSNs; however, existing Internet QoS and MANET QoS mechanisms are not directly applicable to WSNs due to the difference in the characteristics of such networks. In addition, there is currently no standardization in the networking community, on a framework and/or general guidelines on how QoS can be achieved in WSNs. This motivates the need for more research work and efforts in QoS provisioning in WSNs.[3]

III. Challenges In Providing Both Qos And Security For SensorNetworks

The challenges to provide QoS for sensor networks and the difficulties to make sensor networks secure were given previously. All of these challenges apply when one tries to mutually achieve QoS and security for wireless sensor networks. In addition to those, some extra challenges exist in simultaneously

providing security and QoS for WSN applications due to the remarkable interactions between these two concepts. Particularly, degrading effect of security on some QoS parameters complicate the problem of mutual achievement of QoS and security. In this subsection, these additional difficulties related to the security-QoS correlation will be covered. Table 4.1 summarizes the impacts of both concepts on each other and then, these impacts are detailed in the sequel.

A. ***Positive Effects of Security on QoS:*** Availability of a network is the number one requirement to provide QoS guarantees. Simply put, when a network is unavailable meaning that authorized users cannot access the services when needed, the amount of QoS provided by this network can be said to be zero. Although the availability of a network can be harmed by interruption of communication links or failure of some nodes, DoS attacks are the most important threat to service availability. Jamming or energy deprivation attacks described in previous sections may diminish the performance of the network such that expected services cannot be delivered in a healthy way and users/applications receive unpredictable service quality. With a secure system, however, which is resilient to DoS attacks, availability of the network is sustained even under attack, and therefore, QoS can still be guaranteed. As a consequence, security measures preventing DoS attacks contribute to QoS provisioning in sensor networks by Providing availability. In addition, security may help the protection of QoS related network traffic so that planned QoS provisioning techniques can be utilized.[5]

B. ***Positive Effects of Security on QoS:*** The standard approach to provide security to any system is to use of cryptographic primitives such as message integrity codes (MIC), digital signatures, one way hash function, etc. The use of cryptography will mainly have two effects on the performance. The first one is due to the increased overhead in the length of the messages sent and the second one is due to the extra computational demands on the processor. The increased message size causes an increase in packet latency, decrease in throughput and an increased use of available bandwidth. And, the computational overhead results in more latency. These adverse effects are detailed below. The security methods such as MIC or digital signatures append additional bytes at the end of the data packets to be used in verification at receiver's side. These packet overheads are generally in the range of 8-32 bytes and therefore inconsequential for conventional data networks. However, for sensor networks, which have already little bandwidth available to use, packet size is usually small, i.e., 30 bytes in Berkeley's MICA motes. Therefore, a 8-byte security overhead is almost 25% of the total packet size and has several effects on the QoS of the sensor network. Firstly, longer packets occupy more bandwidth leaving less available bandwidth for QoS constrained traffic. Moreover, large packets circulating in the network cause an increase in the total traffic load present in the sensor network. This increased amount of packet traffic may cause congestions on intermediate sensor nodes which forward packets. This congestion not only decreases the average throughput of the network but also causes increased overall delays due to the higher queuing times of congested nodes. The increase in latency is contributed also by longer transmission times of longer data packets. Another element causing degradation of QoS parameters is the computational burden put on the sensor node's processors by cryptographic methods like encryption. Although it varies according to the used cipher algorithm, encryption process usually involves lots of arithmetic and logic operations. These operations take thousands of CPU cycles to be completed by the processor. For Giga-Hertz speed processors used in conventional computers like PCs and laptops, these calculations are not too cumbersome. However, the microprocessors used in generic sensor nodes have much limited capacity. For example, MICA2 motes developed in UC Berkeley possess ATmega128L microprocessors operating at 7.3728 MHz with 128 KB program memory and 4KB data memory. Processing a DES encryption on a 29 bytes payload using these processors take almost one second to complete (Guimaraes et al., 2005). This is a considerable amount of time and greatly affects the packet latency throughout the network. [6]

C. ***Positive Effects of QoS on Security:*** Though it is not as intuitive as for the case of security's effect on QoS, employing QoS mechanisms have some contributing impacts on network security. One of these positive effects cited in Bhattacharya et al. (2000) is the prevention of covert timing channels.

	Effects of Security on QoS	**Effects of QoS on Security**
Positive Effects	**+ Security confirms availability, which is a vital prerequisite for QoS + Security protects QoS related packet headers**	**+ Finely tuned QoS policies can detect and prevent unusual network traffic caused by attacks + Delay bounds provided by QoS may deny covert timing channels**
Negative Effects	**- Security incurs longer packets causing bandwidth consumption and increased delays - Security increases computational load on processors leading more latency**	**- Unprotected QoS labels can leak information about packets in the network - Poorly configured and excessive QoS reservations can deny service to security critical traffic such as key exchange**

A COVERT CHANNEL IS AN UNINTENDED COMMUNICATION CHANNEL THAT MAY BE USED TO TRANSFER DATA IN A MANNER THAT VIOLATES THE SECURITY POLICY. A POTENTIAL COVERT CHANNEL IS A TIMING CHANNEL IF ITS USE INVOLVES A PROCESS THAT SIGNALS INFORMATION TO ANOTHER PROCESS BY MODULATING ITS OWN USE OF SYSTEM RESOURCES (E.G., CPU TIME) IN SUCH A WAY THAT THIS MANIPULATION AFFECTS THE REAL RESPONSE TIME OBSERVED BY THE SECOND PROCESS. IF A QOS POLICY PROVIDES CERTAIN BOUNDS FOR DELAY OR LATENCY, COVERT TIMING CHANNELS CANNOT BE UTILIZED BY MALICIOUS NODES, WHICH IN TURN CONTRIBUTE TO THE SECURITY. ANOTHER POSITIVE EFFECT OF QOS ON SECURITY MENTIONED IN SAKARINDR ET AL. (2005) IS THE FOLLOWING. A FINELY TUNED QOS POLICY THAT PROVIDES CERTAIN AMOUNTS OF BANDWIDTH FOR SOME DEFINED TYPES OF TRAFFIC CAN DETECT UNUSUAL NETWORK TRAFFIC CAUSED BY SOME MALICIOUS NODES THAT ARE LAUNCHING AN ATTACK. IF QOS AND SECURITY SYSTEMS ARE IN COOPERATION AND CAN SHARE INFORMATION, QOS SYSTEM CAN ALERT THE SECURITY SYSTEM ABOUT THE EXISTENCE OF THIS OUT-OF-PROFILE TRAFFIC THAT IS NOT IN ACCORDANCE WITH DEFINED QOS POLICIES, AND THUS HELP THE SECURITY SYSTEM TO DETECT AND PREVENT THIS ATTACK.

D. ***Negative Effects of QoS on Security:*** If QoS mechanisms are poorly configured; they may have detrimental effects on network security. For instance, if critical traffic that is not QoS sensitive is not taken into account while making QoS reservations for services requiring assured delivery, security critical traffic such as key exchange can be denied. Consequently, system security can considerably be Destroyed due to excessive use of QoS mechanisms. Similarly, if the packet headers and other traffic used for negotiating QoS agreements are not properly protected, they may be subject to attacks or at least interference by third parties. In this way, information regarding the importance of packets or other classification levels can leak out. This may provide helpful information for malicious nodes that can be used to launch attacks towards critical points in the network. Thus, unprotected QoS traffic may have negative impacts on network security. The explanations and examples given in this subsection demonstrate that employing security measures on wireless sensor networks positively or adversely affect the QoS parameters and vice versa. Therefore, this complex QoS-security relationship puts additional challenges for the simultaneous achievement of security and QoS for WSN. [7]

IV. Research Methodology

Despite the severe challenges of limited processing power, storage bandwidth and energy, security is important for these devices. These sensors measure environmental parameters and control air-conditioning and lighting systems. Serious privacy questions arise, if third parties can read or tamper with sensor data. In the future these wireless sensor networks will be used for emergency and life-critical systems and there these questions of security becomes foremost. The limited energy supplies create tensions for security: on one hand, security needs to

limit its consumption of processing power, on the other hand, limited supply limits key life time (battery replacement reinitializes devices and zero out the keys).

The aforementioned constraints make the current secure algorithms impractical. For example, the working memory of a sensor node is even insufficient to hold the variables required by asymmetric cryptographic algorithms like RSA It is found that purely symmetric cryptographic primitives (where both parties share a common key) are more suitable for their source constrained sensor networks.

The main objective of this is to improve the Quality of Services in wireless sensor networks on condition that Authentication, authorization, Confidentiality, Privacy and Integrity is maintained in WSN. For this,

1. System uses digital signature for strong authentication.
2. Data Confidentiality using Asymmetric encryption.
3. Privacy and integrity is provided by SafeQ Protocol, a novel and efficient protocol for handling range queries in two-tiered sensor networks. Finally,
4. An extended watchdog mechanism besides the next-hop, node with extended watchdog will monitor all its neighbours' behaviour on the base of information collected from MAC layer.

In the proposed technique we want to improve the Quality of Services of the Wireless Sensor Network by improving the security of the network by using the collaboration of SAFEQ and Watchdog algorithm.

V. Conclusions

In this paper we are proposing the collaborative approach to improve the Quality of Services in Wireless Sensor network by using SAFEQ and Watchdog algorithm. This two algorithms will be used to improve the security of the network as this two algorithm will provide the Security, Privacy and Integrity to the Network, and once we achieve the Security, Privacy and Integrity in Wireless Sensor Network it will going to improve the Quality of Services of the network based on the security parameter. These two algorithms insures that there should not be any unwanted attack on the network and securing the network from unwanted attacker and will improve the Quality of Services.

References

[1] H. O. Sanli, H. Çam and X. Cheng, EQoS: An Energy Efficient QoS Protocol for Wireless Sensor Networks, Proceedings of the 2004 Western Simulation Multi Conference (WMC '04), San Diego, CA, USA, Jan 18 – 21,2004

[2] Tomur and Y.M. Erten, ―Security and Service Quality Analysis for Cluster-Based Wireless Sensor Networks , Fifth International Conference on Wired / Wireless Internet Communications (WWIC 2007), May 2007, Coimbra, Portugal

[3] D. Chen and P. K. Varshney, ―QoS Support in Wireless Sensor Network: A Survey, Proceedings of the 2004 In ternational Conference on Wireless Networks(ICWN2004), Las Vegas, Nevada, USA, June 2004.

[4] M. Sharifi, M. A. Taleghan and A. Taherkordi, ―A Mid- dleware Layer for QoS Support in Wireless Sensor Net- works, Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, Mauritius, 2006.

[5] H. Xiao, W. K. G. Seah, A. Lo and K. C. Chua, A Flexible Quality of Service Model for Mobile Ad- Hoc Networks, Proceedings of IEEE 51st Vehicular Technology Conference, Tokyo, Japan, May 2000.

[6] S. Chakrabarti and A. Mishra, QoS Issues in Ad Hoc Wireless Networks, IEEE Communications Magazine, Feb 2001.

[7] R. Iyer and L. Kleinrock, ―QoS Control for Sensor Net- works, in ICC 2003, Vol. 1, 11-15 May 2003, pp. 517-521.

[8] M.-M. Wang, J.-N. Cao, J. Li and S. K. Das, ―Middleware for Wireless Sensor Networks: A Survey, Journal of Computer Science and Technology, Vol. 23, No. 3, May 2008, pp. 305-326