Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks

Tahir Naeem[1,2], Kok-Keong Loo[1]
[1]School of Engineering and Design, Brunel University, London, UK
[2]Kohat University of Science & Technology (KUST), N.W.F.P, Pakistan
doi: 10.4156/jdcta.vol3.issue1.naeem

Abstract

Both Wireless Mesh Network (WMN) and Wireless Sensor Network (WSN) are multi-hop wireless networks. WMN is an emerging community based integrated broadband wireless network which ensures high bandwidth ubiquitous internet provision to users, while, WSN is application specific and ensures large scale real-time data processing in complex environment. Both these wireless networks have some common vulnerable features which may increase the chances of different sorts of security attacks. Wireless sensor nodes have computation, memory and power limitations, which do not allow for implementation of complex security mechanism.

In this paper, we discuss the common limitations and vulnerable features of WMN and WSN, along with the associated security threats and possible countermeasures. We also propose security mechanisms keeping in view the architecture and limitations of both. This article will serve as a baseline guide for the new researchers who are concern with the security aspects of WMN and WSN.

Keywords

Multi-hop, Wireless Mesh Network, Wireless Sensor Network, Security

1. Introduction

Security aspects of multi-hop wireless networks such as WMNs and WSNs are gaining interests of researchers as there are still numerous unresolved issues which needed to be addresses before large scale exploitation take place. WMN is an integrated broadband technology which not only provides high bandwidth internet facility to users but also integration of other wired and wireless networks such as IEEE 802.11, IEEE 802.16, IEEE 802.15, and LANs. Special features of WMN include its low cost, easily deployable, self-healing and self-configuring network. WSN is purpose-based application-specific wireless network which ensure large scale real time data processing in complex environment. Few applications of WSN are traffic controlling, habitat monitoring, flood informing, health care etc. However, both these tremendous wireless networks face critical security challenges due to their few vulnerable characteristics, which the attackers try to exploit and bring serious performance degradation. Three common security requirements for any wireless networks are confidentiality, data integrity and service availability [5]. Confidentiality deals with end-users traffic and it ensure that the traffic is not listened or viewed by any entity except the intended recipient. Confidentiality is protected by using strong authentication and encryption mechanisms. Data integrity ensures that the packets are received by the receiver in the same format and sequence as sent by the sender, here the purpose is to keep the attackers away from packets modifications, alteration, disruption and absorption. Data integrity is mostly dependent on the underlying routing protocols. Availability is the feature which makes sure that the network and network resources are always available to end-users without any delay or interference. Three major types of security threats have been observed in wireless networks especially multi-hop wireless networks such as WMN and WSN, i.e. passive, active and DoS security threats. Passive attacks compromise the confidentiality by stealing information over the wireless medium using tools like sniffers. Passive attacks are very difficult to detect as they are silent in nature and do not harm the network. Active attacks compromise the data integrity by modifying, tempering, altering the packets. Such attacks mostly exploit the weaknesses in routing protocols. DoS

attacks compromise availability by reducing or stopping the network services and resources to legitimate users. The multi-hop wireless networks are more vulnerable to all these security attacks and exploitations. Being a broadband wireless network, the security of WMN is highly important as it is directly providing services to hundreds and thousands of end-users. At the same time, we cannot overlook the security aspect of WSN, as medical monitoring, industrial automation and military applications emphasize the need to secure the sensor networks. There is a real need to address the security related issues prior to the commercial deployment of such multi-hop networks. We propose security mechanisms exclusively for WMN and WSN, keeping the limitations and challenges of these networks. Our proposed security system for WMN is based on detects and response, i.e. detect the intrusion and take appropriate action. The proposed security system for WSN is a security agent in the gateway, as gateway is the most important component of sensor networks, as all the traffic from the sensor node is routed to sink through the gateway.

This article presents three principal findings. First, the common vulnerable characteristics of WMN and WSN are pointed out. Second, all possible security attacks and possible defenses are described. Finally, we propose two security mechanisms for WMN and WSN.

2. Common vulnerable features of WMN and WSN

WMN and WSN are both multi-hop infrastructure-based wireless networks; however both have significant different purposes and objectives. WMN is integrated broadband wireless network which not only ensures high bandwidth internet provision to the end users but also form integration between other wired and wireless networks such as LANs, WLANs, WMANs and cellular networks. The important special features of WMN are its self-healing, self-configuring, easy deployment, low cost and de-centralized architecture.

WSN is application specific and are specially designed to serve in emergency environments such as battle field, flood alarming, habitat monitoring, health care etc. sensor nodes are generally small in size having little memory and computation power, and are densely deployed in the coverage area so that to get accurate results and figures.

WMN perform three levels of operations for internet provision to the end users, i.e. the gateways form the top-levels and are connected with the wired network infrastructure for internet access. The middle levels constitute the mesh routers which form the multi-hop structure for giving access to the end-users. End-users mesh nodes form the lowest level. Two types of mesh nodes exist in WMN, one type of mesh nodes are directly connected with the mesh routers if they are in the direct communication range of mesh routers, if some nodes are not in the direct communication range of mesh routers, then WMN support the ad-hoc connectivity amongst the mesh nodes, i.e. the mesh nodes can connect with the wireless network trough other mesh nodes.

WSN operates in the same level, i.e. there are no particular routers or gateways; however all the nodes communicate with each other having router's capabilities for relaying data for each other. Few of sensor nodes may perform the gateways functionalities and all the nodes send the collected data towards the sink through the gateways. Sink is a repository, which keeps all the collected data and figures to scientifically predict the outcomes.

Although, the physical setup, topologies, operations and routing mechanisms are different in WMN and WSN, but still both posses some common vulnerable characteristics and security challenges which may compromise the confidentiality, data integrity and service availability, and are mention in this section.

A. Wireless Medium

Both WMN and WSN use frequency band for wireless communication. In WMN, mesh nodes are either connected wirelessly with mesh routers or another mesh node using 2.4 GHz free frequency band.

In WSN, nodes are connected with each other, and the traffic pattern is toward the sink through the gateways, uses variable bands of frequency depending upon the nature and type of application, as for example, the WSN used for animal tracking or habitat monitoring uses 174 MHz, while most of the alarming sensor nodes use 434 MHz frequency band.

Jamming and scrambling are common security threats for the wireless medium of WSN and WMN. In jamming, the attacker uses a specialized hardware device to introduce a strong noise so that to create serious interference in the communication channels [1]. Scrambling is periodical short term jamming in which the strong noise is introduces after specified interval of time, hence the communication channels of wireless

medium work for some time and stop working during the period of scrambling.

As a whole jamming and scrambling is used as a weapon against the wireless networks particularly in WMN and WSN, it can be used for jamming

- Mesh nodes to isolate them from network services and resources.
- Mesh routers to isolate a portion of network.
- Mesh gateways to completely bring down the broadband services and resources.
- Sensor nodes to isolate them from the rest of the network.
- Sensor gateways to stop the traffic flows toward the sink.

Here the low intensity jamming attack is against the sensor and mesh nodes, while the most severe type is the jamming attack against the mesh and sensor gateways, as jamming gateways mean that the complete network is down.

In wireless networks, the strategy is that to keep the location of the gateway hidden so that to prevent the physical damage and jamming kinds of attacks, as gateways are the core and most important backbone devices. However, the attackers locate the gateways [3] by first conducting a passive homing attack. In homing attack, the intruder passively monitors and observes the traffic pattern in the network, as in both WMN and WSN; the traffic pattern is from nodes toward the gateways. After successful homing attack, now the attacker is aware of the gateways locations, and hence jamming is possible.

B. Cooperative MAC

Both WMN and WSN use cooperative MAC (Medium Access Control) protocol at data link layer, which is shared amongst all the nodes in communication. This cooperative MAC gives rise to hidden node terminal and collusion of packets. For example, nodes A and B are in the communication range of C, but A and B are not in direct communication range of each other, that is why, nodes A and B are not aware of each other, and both want to send data through node C, here either both will transmit simultaneously and hence packet collision would occur, or node A is communicating with node C, hence node B is unable to transmit its data unless node A has finished the session. Ready To Send / Clear To Send (RTS/CTS) mechanism was introduced to solve the problem of hidden node terminal, as first the node would send a RTS signal to the communicating node, and if received the CTS signal, which means that no any other node is transmitting the data, hence the node can transmit the data. However, MAC with RTS/CTS still faces the problem of exposed node terminal, which needs to be resolved.

In WMN and WSN, the attackers exploit the cooperative MAC with RTS/CTS for launching many security attacks.

- The nodes can flood the packets of RTS toward the target node, as a result the target node will reply to each of the RTS with CTS, hence creating extra overheads on the bandwidth, computation processing and power consumption.
- The malicious node can capture the MAC channel for indefinite period and continuous transmission; hence other nodes are unable to participate in the communication process.
- The exposed node problem is still not fully solved, and if a malicious node acts as an exposed node, it can stop the communication process of innocent nodes.

The cooperative MAC and the RTS/CTS mechanisms can seriously degrade the performance of WSN as compared to WMN. The data received in WSN are mostly dependent on the observation and the captured information of the sensor nodes; hence the results of the received data can be seriously corrupted if the strategically important nodes in WSN become the victim of selfish MAC behavior, and are unable to communicate.

C. Multi-hop environment

Both WMN and WSN are multi-hop wireless networks. Data traffic passes in hop by hop pattern toward the destination. Multi-hop architecture is necessary for easy and rapid deployment, as well as it also reduce the deployment cost, as the nodes have the flexibility of self-healing, self-configuring and self-adjusting. This feature also greatly increase the reliability, as there exist many paths between the source and destination, and in case of any path failure, there exists alternate paths between source and destination to carry out the communication. On the other heads, this feature also has three negative aspects;

- Routing overheads increases
- Security risks increases
- Bandwidth decreases

The main security threats due to the multi-hop nature of

WMN and WSN are

- Blackhole attack [6], in which the malicious node drops all the traffic.
- Greyhole attack, in which the malicious nodes selectively drop the network traffic
- Wormhole attack [7], in which two distant malicious nodes form a fast communication link, capture the packets at one end, forward to the other through the fast link, and replayed the packets there to create routing disruption [6].
- False route creation attack, in which malicious nodes create false and non-existing routes between source and destination.
- Sybil attack, in which a malicious nodes show many identities at a time, so create routing loops [8].

These multi-hop routing attacks can be of serious consequences if launched against WSN in emergency situations such as health care or battle field. However, the severity of such attacks will be worst if the blackhole or greyhole malicious nodes exist near the gateway of the WSN, hence, most of the traffic would be either dropped or selectively forwarded to the sink.

D. Power limitations

As WSN consist of tiny nodes, which have limited or definite battery power. The sensor nodes conserve the energy by going to sleep-mode when there is no data to transmit. The energy consume when sensor nodes transmit the data, hence their radios are on for this purpose.

In WMN, the mesh nodes may be static or mobile. Generally static nodes have no power limitations; however the mobile mesh nodes have power constraints.

The attackers can seriously degrade the performance of WSN, if strategically important nodes are under sleep-deprivation attack [9]. In this attack, the attacker's usually forward un-necessary packets towards the target node so that to keep its radios on, hence consumes its battery power to completely drain and makes it unable to take part in the communication process.

The WSN has serious concerns regarding power limitations as compared to WMN nodes, as in WSN, all the nodes are power constrained, which is not the case in WMN.

As WMN support both static and mobile nodes, here the mobile nodes have limited supply and life of battery, however, if any mobile node of WMN is under sleep deprivation attack, it is of less severity and consequences limited to the mobile node only, i.e. the network operations remain unaffected.

The limitations, attacks and possible defenses are given in Table 1.

Table 1. Limitations, security concerns and possible defenses

Limitations	Security concerns	Defenses
Wireless Medium	Jamming	Spread spectrum Frequency hoping
Cooperative MAC	Selfishness	Multi-radio multi channel Cognitive radios IEEE 802.16 mechanism
Multi-hop	Blackhole, greyhole, Rushing, Sybil	Secure routing protocol
Power	Sleep deprivation	IDS agent

3. Possible research directions

Some facts needs to be considered before designing and proposing any security mechanism for WMN, such as

- As a large scale broadband network, WMN consists of fixed backbone mesh routers and gateways infrastructure, which is not power constraint.
- Majority of mesh nodes are static which have no power limitations; however there is also support for mobile nodes.
- WMN is an integrated technology, which can enable integration amongst other wireless networks such as IEEE 802.11 WLANs, IEEE 802.16 WMANs.
- In WMN, most of the traffic is from gateways toward the users for Internet services.
- Throughput reduction for longer hop communication

For WMN, there is a need of such security mechanism, which considers the three level operations as discussed earlier. The lower level mesh nodes and the middle level mesh routers are more vulnerable to most of the security attacks. Any proposed solution should be defined by adapting the fundamental operational nature of the WMN, the proposed security systems must meet the security requirement and

perform well in the multi-hop, large scale, integrated broadband environment of WMN.

In case of WSN, some important facts needs to be considered before designing and proposing any security mechanism such as

- As an application specific network, WSN consists of hundred and thousands of sensor nodes densely deployed in the sensor field.
- Majority of sensor nodes are static having power limitations.
- In WSN, most of the traffic is from node to nodes toward the sink through the fateway gateways.
- The security of the gateway is much more important than the nodes, as all the traffic passes through the gateways.
- The low memory and computation power limits the scope of heavy security mechanisms.

Keeping in view the characteristics, multi-hop architecture, dynamic topologies of WSN and WMN, some sort of security mechanisms needs to be investigated which are capable to ensure secure communication. Some possible research directions are listed below.

- The advance anti-jamming techniques such as frequency hopping and spread spectrum are the best solution to prevent jamming and scrambling attacks. However, these solutions can only be used in WMN, but not practical for WSN. The WSN nodes are lower power, low cost, and these techniques require high energy consumption and increase the design complexity [2]. One solution can be to put the sensor nodes in sleep mode and wake them after some time to check that the jamming attack is still in existence or ended so that to increase the battery life of the sensor nodes, however this cannot prevent the DoS attack [3]. One of the possible mechanism to protect WSN against jamming is the investigation of jamming-detection and alarming mechanism in few of the superior sensor nodes having more memory, computation and power resources than the others, and are deployed around the boundary of sensor field so that to sense the jamming attack and to inform the appropriate person. This kind of mechanism would be helpful to mitigate such attacks and avoid large scale exploitation.
- Some mechanisms needs to be investigated for WSN and WMN so that to eliminate the factor of selfish MAC. For WMN, IEEE 802.16 MAC mechanism can be consider, which uses TDMA and TDM for uplink and downlink, and ensure collision free transmission. Multi-radio multi-channel could also be a good candidate in WMN to be considered and investigated. Cognitive radio design and implementation is another potential area to be evaluated [4]. In WSN, there is a need to reduce the chances of indefinite channel capturing and RTS/CTS flooding attack, and are highly challenging research area.
- To overcome the overheads of multi-hop in WSN and WMN, the most efficient solution would be the implementation of secure routing protocol which is capable of secure-path selection, and which is proposed keeping in view the limitations and challenges imposed by the multi-hop complexity.
- Most of the serious attacks in WMN and WSN can be countered by using Intrusion Detection System (IDS), which is capable to detect the intrusion and inform the appropriate controller for action. However, the IDS design must consider the complexities and challenges of WMN and WSN environment, also the accuracy and timely detection of any risk are the key factors of secure IDS. For WMN, the IDS can be implemented either in mesh nodes to individually counter the security attacks, or can be implemented in mesh router to monitor all the in-range mesh nodes for misbehavior. In WSN, due to its inherit limitations regarding memory, power and computation, individual IDS in sensor nodes are practically not possible, however, the research community may try to investigate an IDS for the sensor gateways, which is capable to monitor the surrounding nodes of the gateway for misbehavior.

4. Conclusions

Both WMN and WSN are multi-hop wireless networks having some common limitations and challenges. The open wireless medium, multi-hop architecture, power restrictions and cooperative and shared MAC are such characteristics which impose

many security challenges in them. The security challenges may be physical threats such as jamming and scrambling, MAC related risks such as MAC selfishness or exploitation of RTS/CTS mechanism, routing attacks such blackhole, greyhole, sybile, and sleep-deprivation attacks to drain the power resources. Spread spectrum, frequency hopping, or cognitive radios may be considered to prevent the jamming attacks, but these techniques are not suitable for WSN due to the simplicity and low power of the sensor nodes. Routing attacks due to the multi-hop architectural complexity can be solved by secure routing protocols for WSN and WMN. Intrusion detection system can be a good candidate to be considered for these multi-hop wireless networks, however, such mechanism may not be more feasible for WSN; as such mechanism may increase the design complexity of sensor nodes, however can be investigated for sensor gateways. There is a real need for such security mechanism which are proposed and designed keeping in view the limitations and challenges of WSN and WMN.

5. References

[1] S. Khan, K-k. Loo, T. Naeem, M.A. Khan, "Denial of service attacks and challenges in broadband wireless network," International Journal of Computer Science and Network Security, Vol. 8, No. 7, pp.1-6, July 2008.

[2] Y. Wang, G. Attebury, B. Ramamurthy, "A survey of security issues in wireless sensor networks," IEEE Communications Surveys and Tutorials, Vol. 8, No. 2, pp. 2-23, 2006.

[3] D.R. Raymond, S.F. Midkiff, "Denial of service in wireless sensor networks: attacks and defenses," IEEE Pervasive Computing, Vol. 7, Issue 1, pp. 74-81, 2008
.

[4] R. Venkatesha Prasad, P. Pawtczak, J. A. Hoffmeyer, and H. S. Berger, "Cognitive functionality in next generation wireless networks: Standardization efforts," IEEE Communication Magazine, Vol. 46, Issue 4, pp. 72-78, April 2008.

[5] F. Xing, W. Wang, "Understanding Dynamic Denial of Service Attack in Mobile Ad hoc Networks," IEEE Military communication conference (MILCOM), 2006.

[6] Y. Wang, G. Attebury, B. Ramamurthy, "A survey of security issues in Wireless Sensor Networks," IEEE Communications Surveys & Tutorials, Vol. 8, No.2, 2006.

[7] F. Nait-Abdesselam, B. Bensaou, T. Taleb, "Detecting and avoiding wormhole attacks in wireless Ad hoc networks," IEEE Communication Magazine, Vol.46, Issue 4, pp. 127-133, April 2008.

[8] Y. Zhang, J. Luo, H. Hu, "Wireless mesh networking, architectures, protocols and standards," Auerbach Publications, Taylor & Francis Group, First Edition, NY, ISBN: 0849373999, 2006.

[9] M. S. Siddiqui, C. S. Hong, "security issues in wireless mesh networks" IEEE International Conference on Multimedia and Ubiquitous Engineering(MUE'07) 2007.