Bikram Pratap Singh, et. al. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 16, Issue 3, March 2026, pp 13-16

RESEARCH ARTICLE OPEN ACCESS

"Security issues across different layers of the WSN architecture"

[1]Bikram Pratap Singh - *Research Scholar*
Faculty of Engineering & Technology
ASIAN INTERNATIONAL UNIVERSITY
IMPHAL WEST, MANIPUR

[2]Dr Sanjay Kumar- *Professor*
Faculty of Engineering & Technology
ASIAN INTERNATIONAL UNIVERSITY
IMPHAL WEST, MANIPUR

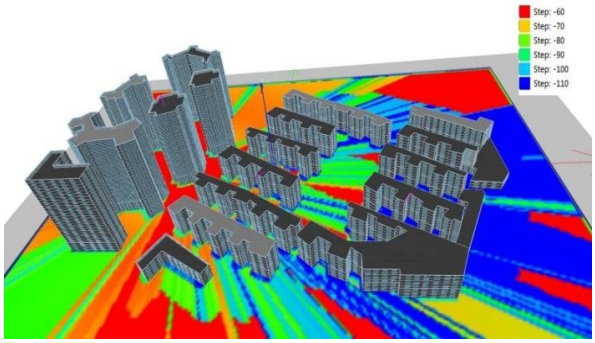
ABSTRACT
Wireless sensor networks (WSNs) have become one of the current research areas, and it proves to be a very supportive technology for various applications such as environmental-, military-, health-, home-, and office-based applications. WSN can either be mobile wireless sensor network (MWSN) or static wireless sensor network (SWSN). MWSN is a specialized wireless network consisting of considerable number of mobile sensors, however the instability of its topology introduces several performance issues during data routing. SWSNs consisting of static nodes with static topology also share some of the security challenges of MWSNs due to some constraints associated with the sensor nodes. Security, privacy, computation and energy constraints, and reliability issues are the major challenges facing WSNs, especially during routing. To solve these challenges, WSN routing protocols must ensure confidentiality, integrity, privacy preservation, and reliability in the network. Thus, efficient and energy-aware countermeasures have to be designed to prevent intrusion in the network. In this chapter, we describe different forms of WSNs, challenges, solutions, and a point-to-point multi-hop-based secure solution for effective routing in WSNs. Wireless sensor network (WSN), as shown in is a wireless interconnected network which consists of independently setup devices that monitor the conditions of its environment using sensors. WSNs are employed in a wide range of applications such as security surveillance, environmental monitoring, target tracking, military defense, intrusion detection, etc. Security in wireless sensor network is at a growing stage mainly not because of nonavailability of efficient security schemes, but most of the existing schemes are not suitable due to the peculiarity of WSNs. That is, WSNs' nodes have low computational capacity and energy constraint. In WSNs, sensor nodes have the ability to communicate with one another, but their primary task is to sense, gather, and compute data. These data are forwarded, via multiple hops, to a sink which may use it or relay it to other networks. To achieve an effective communication, WSNs need efficient routing protocols. They facilitate communication in WSNs by discovering the appropriate routes for transmitting data and maintain the routes for subsequent transmissions. As a result of heterogeneity of WSNs' nodes, different protocols had been developed for different WSNs depending on the nature of the nodes and application. For instance, there are dedicated protocols for MWSNs and dedicated protocols for SWSNs. There are two modes of transmission in WSN; single hop involves the source node sending its data packets to the destination within a hop. Meanwhile, WSNs' sensor nodes may rely on one another in order to relay packets to remote destinations. This mode of transmission is called multi-hop. Multi-hop is a routing phenomenon that involves the transfer of data between source and destination nodes with the cooperation of intermediary nodes. It enhances the performance of WSNs by allowing energy-depleted node to transfer data through its neighboring nodes along the routing path to the destination node. There are several security and privacy issues associated with multi-hop routing. Some of these issues like snooping, sinkhole, tampering Sybil, clone, wormhole, spoofing, etc. affect the integrity, availability, and data confidentiality of the WSNs.
Several security solutions had been proposed for WSNs; however, resource constraint of sensors makes some of these security solutions unfit for WSNs. This, therefore, makes their adoption in WSNs impossible. This is as a result of instability of the topology of most WSNs. Some of the WSNs, unlike some other networks, consist of mobile nodes that intermittently change the topology of the networks, therefore making it impossible for such mobile network to use existing protocol developed for static nodes. Also, large volume of data is transferred on the WSNs; this increases the traffic on the wireless communication infrastructure of WSN. All these show that security and privacy solutions of WSN must not only be lightweight in terms of the computational, communication, and energy overheads but also support aggregation and multi-hop in order to reduce the traffics and extend the life span of the networks. Meanwhile, most of the existing security solutions do not have these performance requirements
Keywords: WSN, networks, MWSN, wireless, sensor, mobile

I. Introduction

Inside attackers can damage the network stealthily since they can avoid our authentication and authorization because they are legitimate nodes of the native network and have access to the network information, and it is not easy to expect their attack patterns. Inside attackers can launch various types of attacks, such as modification, misrouting, eavesdropping or packet drop. This last attack is tricky to counter, because for a particular packet drop, we cannot distinguish whether it is dropped by an attacker or a result from collision or noise. This attack suppresses the important information reaching the base station which significantly degrades network performance, such as packet delivery rate due to their repeated packet drops. There are several types of packet drop attacks such as blackhole, grayhole and on-off attacks. This is a serious threat for many applications, such as military surveillance system that monitors the battlefield and other critical infrastructures. The functionality of link layer protocols is to coordinate neighboring nodes to access shared wireless channels and to provide link abstraction to upper layers. Attackers can deliberately violate predefined protocol behaviors at link layer. For example, attackers may induce collisions by disrupting a packet, cause drain of sensor node energy by repeated retransmissions, or intercepting and examining messages in order to deduce information from patterns in communication. This can be performed even when the messages are encrypted and cannot be decrypted, or even cause unfairness by abusing a cooperative MAC layer priority scheme However, they do not deal with key refresh which makes key management dynamic and adds a further difficulty to the task of attackers. Furthermore, symmetric solutions do not scale well when the number of sensor nodes increases, and neglect the effect of captured node attacks.

Coverage gaps of cellular network in outdoor.

Using symmetric cryptographies in software implementation are challenging. Because they are not providing a perfect trade-off between resilience and performance, and hostile nature environments where sensor nodes are deployed makes it vulnerable to various attacks. In the context of public-key cryptography, with thousands and millions of multiplications involved, it has become a major research branch to adapt and optimize advanced cryptosystems to small systems, such as sensor devices. Many works focused on the lightweight adaption of asymmetric cryptographic algorithms. The wireless sensor networks continue to grow and become widely used in many mission-critical applications. So, the need for security becomes vital. However, the wireless sensor network suffers from many constraints such as limited energy, processing capability, and storage capacity, as well as unreliable communication and unattended operation, etc. There are many ways to provide security, and the main one is cryptography. Selecting the appropriate cryptography method for sensor nodes is fundamental to provide appropriate security services in WSNs. Public-key cryptosystems are considered to be too heavy for resource-constrained sensor nodes. However, several studies have shown that it is feasible to apply public key cryptography to sensor networks by using the right selection of algorithms and associated parameters, optimization, and low power techniques. These cryptographic schemes were introduced to remove the drawbacks of symmetric based approaches, and lead to more performance.



II. Methodology

Based on the analysis of existing methods and practices in the humanitarian mapping community, we would like to frame the production of urban community data as an interdisciplinary methodological challenge as illustrated. The methodological challenge consists of designing a process that can provide rigorous evidence for policy and decision-making, whilst at the same time effectively promoting inclusive and empowering relations with the communities involved. This involves a dialogue with two different perspectives on mapping. Traditional mapping techniques (e.g. such as those used by geometrics companies and national mapping agencies) can produce spatial data with a high degree of adherence to spatial data quality standards. They follow strict guidelines and aim at a well-defined set of dimensions of spatial data quality (e.g. completeness, logical consistency, positional temporal and thematic accuracy). However, the application of these methods is costly and the technical expertise required excludes inhabitants from the poor urban communities from the process. In contrast, participatory mapping techniques (as the ones used in the humanitarian mapping community) are a good way to engage residents and local stakeholders in thinking differently about their relationship with the environment and the urban

space; but as previously seen the extent to which the resulting data matches quality requirements is often uncertain. Operating at the intersection of these two mapping traditions, we see an interdisciplinary problem space that is associated with a twofold methodological challenge:

(a) promote effective engagement and participation of local stakeholders and residents of urban communities, with the goals of building capacity, empowering them for creating local ownership and ensuring the sustainability of the geographic data generated;

(b) Assess and improve spatial data quality, in order to ensure that the resulting data is able to capture intra-urban inequalities and be used as trusted evidence for scientific research and policy making. To tackle this challenge, our methodological approach is based on participatory and collaborative mapping, but in addition to the methods adapted to by similar initiatives; the present approach introduces further steps of data production and validation to maximize spatial accuracy, whilst simultaneously engaging community members. Given the high density of poor urban neighborhoods such as slums and their morphological variety across countries using a methodology which is sensitive to the contextual characteristics is of crucial importance to creating a base for representative urban policies. The ultimate scope of this research is to propose a roadmap for systematic but context-aware participatory mapping of disadvantaged communities.

III. Results

Both RSA and Diffie-Hellman based on the elliptic curve cryptography are possible for tiny sensor nodes, and the results show that it is possible to achieve good results with smaller keys. It reduces computation time and also the amount of data transmitted and stored. Asymmetric approaches with public key cryptosystems, specifically elliptic curve cryptography are promising approach for meeting security requirements in WSNs. In this article, we aimed to provide a general overview of the major aspects of wireless sensor networks security: challenges, goals, and attacks; as well as some of commonly used defenses approaches. our intervention (based only on satellite imagery), most of them needed further mapping and validation, as their accuracy has proven to be variable after verification on the ground. Interesting information regarding the quality of spatial data, which emerged from our mapping and validation process? It is noticeable that the spatial data, namely structures and roads, within examined slum areas have increased significantly as a result of our project. Even in communities such as Korogocho (Nairobi), where there was previous data and the number and length of roads seem to have been reduced, the overall accuracy and precision of the spatial data has been largely enhanced. The numbers in, with the exception of Kraal, are the result of online mapping and validation processes, as ground-trotting activities have not been performed so far show the previous data (small inlet map) and current status (larger map) of some of the mapped communities.

IV. Conclusion

Public-key cryptosystems are considered to be too heavy to use in WSNs. However, recent works show successful implementation examples of public-key cryptography in constrained sensors devices. In Gura et al. report that both RSA and elliptic curve cryptography are possible for small devices without hardware acceleration. With 8-bit CPUs, ECC shows a performance advantage over RSA. Another advantage is that ECC's 160-bit keys result in shorter messages during transmission compared to the 1024-bit RSA keys. In particular, Gura et al. demonstrate that ECC point multiplication on small devices is comparable in performance to RSA public-key operations and an order of magnitude faster than RSA private-key operations. In Watro et al. show that part of the RSA cryptosystem can be successfully applied to actual wireless sensors. The TinyPK system described by is designed to allow authentication and key agreement between resourceconstrained sensors. The protocol is used together with the existing symmetric encryption service for node networks, such as, TinySec. In particular, they implemented the RSA public operations on the sensors and the RSA private operations to an external party, such as a laptop. In Malan et al. demonstrate a working implementation of Diffie-Hellman based on the Elliptic Curve Discrete Logarithm Problem. In addition, they show that public keys can be generated within 34 seconds, and that shared secrets can be distributed among nodes in a sensor network within the same, using just over 1 kilobyte of SRAM and 34 kilobytes of ROM. So, public-key infrastructure is viable on the MICA2 for infrequent distribution of shared secrets. Wang et al. in proposes a public-key scheme for WSNs. They built an ECC-based access, which consists of pairwise key establishment, local access control, and remote access control. They have performed a comparison test by implementing both symmetric-key and public-key primitives on MICAz nodes and HP iPAQ. Their case study shows that the public-key scheme is more advantageous than symmetric key in terms of the memory usage, message complexity, and security resilience.

Reference

[1]. I.F.Akyildiz et al., "A Survey on Sensor Networks", IEEE Commun.Mag.,Vol. 40, No. 8, pp.102-114, Aug. 2002..

[2]. Salgado de Snyder VN, Fried S, Foots JC, Chard Z, Marksman S, Monger P, Patil-Deshmukh A. Social conditions and urban health inequities: Realities, challenges and opportunities to transform the urban landscape through research and action. Doi: 10.1007/s11524-011-9609-y.

[3]. Fried S, Ackerman M, Hancock T, Kumaresan J, Marmot M, Melina T, Vlahos D; GRNUHE members. Addressing the social and environmental determinants of urban health equity: evidence for action and a research agenda. Doi: 10.1007/s11524-011-9606-1.

[4]. Fried S, Hancock T, Kjellstrom T, McGranahan G, Monger P, Roy J. Urban Health Inequities and the Added Pressure of Climate Change: An Action-Oriented Research Agenda. Doi: 10.1007/s11524-011-9607-0.

[5]. Bartend F, Ackerman M, Becker D, Fried S, Hancock T, Mwatsama M, Rice M, Shauna S, Stern R. Rights, knowledge and governance for improved health equity in urban settings. Doi: 10.1007/s11524-011-9608-z.

[6]. World Health Organization. http://1000cities.who.int/. Accessed May 15, 2011.