Id-base encryption in wireless sensor networks

Hosseini, Abed[1]

Department of computer science, Islamic azad university, Ayatollah Amoli Branch,Iran

hosseini_abed@yahoo.com

Abstract— The use of wireless sensor networks, especially in the past decade has increased dramatically. This network is composed of a large number of the small sensor would have been an efficient tool to collect data from the environment. The data collected by the sensors is transmitted to the base station will eventually be available to the end user data. Key management is one of the most important topics in WSN limited resources because the sensor nodes using the normal security techniques. The sensor network more than a shared between all nodes will use the communication overhead at a minimum. But this method compared to the many attacks like theft, attack attack, run again confirming (replay) attacks the lack of compromise, etc., is vulnerable. In this article, we have a number of cryptographic methods for providing wireless sensor networks have been described, and then a comparison between these methods do.

Keywords: *wireless sensor networking, WSN, encryption, security,*

- ***INTRODUCTION***

Introduction: wireless sensor network, a distributed system, which is an autonomous and organizer of many sensor nodes is small with the little operational need that energy [1]. The sensor nodes have restrictions on energy resources, computational and processor. These networks in cases such as the monitoring of environmental conditions, time, collect data, such as temperature and pressure, and military applications [2]. The application of. The disadvantage of this approach is that if a node is a communication link, the capture of which is not directly associated with captive also affects. Wireless network encryption when the need to configure each network component is a complex task. First and foremost the encryption starting point is where the local network can be connected to the Internet. With the use of encryption of your data within and outside of the network can read and work is difficult for hackers and theft. In the past, organizations, and companies that need to encrypt the encryption or other services, the unique design of the encryption algorithm. Specifies the time that a huge security weakness in these sometimes algorithms that exists by virtue of the ease of getting broken password. That's why today, cryptography-based keep hidden encryption algorithm is outdated and a new method of encryption, it is assumed that complete information encryption algorithm has been published. Due to the variety of sentences and security services needed to deal with this security policy is an integrated design for any attacks on the network is very essential. Taking into consideration the limitations that wireless sensor networks are faced with it and things like extensibility, communication overhead, a leading privacy and variety of solutions offered, psaro. With the advancement of the technology of public key-based methods with a lot of computational overhead but are still top of the methods permitted in front of the increasing application of these methods. Therefore, try to be more than the combined method is used.

- ***Encryption methods***

✓ ***Wired Equivalent Privacy (WEP)***

This encryption method is introduced as the first method. This method is a low-security level. In this way we enter password network settings so that only for people who have the password can be used. But this method is very time-to consume because you must enter the password manually. And the other problem is that short of being lists of ways to easily identify the codes. The reason why this method very high security because it will.

✓ ***Wi-fi protected Access***

The procedure for the use of wep is used. This method on the data contained in the packaging, and the structure of the network must be sure of our device settings on the standard WEP data encryption, otherwise, we will remain on. This method uses the Protocol (TEMPORAL key integrity protocol), Tkip changes the code.

https://sites.google.com/site/IJCSWN/
ISSN 2519-0814

✓ ***Media Access control (MAC)***

This security method is suitable for small networks because networks that are a great possibility to address this very problem of the access point.

✓ ***WPA***

This is the second method and more advanced protection. In this option, which stands for wi-fi protect access is your connection to your modem you protection as follows: make sure the model has 3 data encryption mode.

✓ ***WPA2***

This method is WPA method on how to encrypt information to send to the destination. This method is the most powerful method for encryption. This method is currently the most common methods [3].

- ***Comparison of encryption methods***

WEP encryption is now based, is but one of the WPA Protocol is used for encryption.
Protocol WEP in less than ten minutes can be broken, but scrambled breaking WPA key with a 21-bit more than 4 × 1020 takes years. WEP can only 64 icons, 128, 152-bit IV (Initialization Vector) and a similar or the same primary icon vector production uses encryption, but in a complex of two WPA encryption algorithm called TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) is used in the layout of each generated dozens of times and encryption company info and are destroyed.
The length of the vector is twice the WEP IV. IV in the definition of the five trillion more key WPA to provide comparisons, but this number is approximately 7.16 million in WEP key.
WPA encryption protocols as one of the two modes will be examined.
(Pre-shared, WPA2) and WPA2 (PSK – WPA2) for general tasks, which according to the needs of selected workstation security level than WPA2.
Dare we can say that a higher level of security than WPA2 to WPA encryption and is entitled to the full implementation of the (802, 11i) is a subset of the standards of securing wireless networks WPA and WPA at any time by the work of hackers actually do protection work, WPA2. It must be said that WPA2 AES is by definition very much stronger than TKIP.
TKIP for WPA.
TKIP and AES encryption are two different methods that can be used to secure WiFi networks.[4]

AES = Stands for Advanced Encryption Standard

In this case, the modem encryption using the advanced technology of its connection with the device you want to have that connection with encryption.
In a nutshell, TKIP encryption standard is an old order that for the older standard called WPA AES also used a newer encryption solution. is provided by a new and more secure WPA2 standard.
In a nutshell, TKIP encryption standard is an old order that for the older standard called WPA AES also used a newer encryption solution. is provided by a new and more secure WPA2 standard.
Perhaps it is interesting to know that the options compatible with WPA and TKIP can speed your WiFi network to reduce appreciably form. A lot of new routers that use the communication standards 802.11 n and faster and newer standards support, enable WPA or TKIP darshan in your options, 54 Mbit/s will be reduced. This slow down in order to ensure compatibility with older devices.
If the router has 802 .11n from WPA2 AES, alongside the fast up to 300 Mbit/s will support. The 802.11 standard, such as in the case of ac this very difference speed will be more egregious because the standard in terms of theory and is in perfect condition, the maximum speed of Gigabit/s 3.46 support.[5]
In other words, regardless of the topic of security, in terms of the speed of the communication network of the old standards as well as the use of WiFi WPA and TKIP is not in any way logical.
But what is certain is that in most routers available in the market in Iran and in particular FTP links and routers that link over other brands among Iranian users metdaoland, access is the ideal option IE WPA2-PSK-AES is predicting.
If your router WPA2 offers to you, be sure to choose AES. Be sure your device is compatible with it often and your imagination, as well as the rest of the security and the speed, will be. So always keep in mind that the choice of what AES encryption standard to encrypt connections WiFi and what to encode any type of other information such as hard drives, security and will bring more speed.

Select the type of security encryption for wireless sensor networking is very important, especially because now hacking can be done easily and a lot of free software out there for this purpose that easily can be used to break the network key to use them. Securing the Wifi network password the first step to the creation of the security. With the SQL password for the Wifi network in minutes can be used to establish relative

https://sites.google.com/site/IJCSWN/
ISSN 2519-0814

security to WPA2 for security so that this network is recommended.

Comparison chart [6]

WEP versus WPA comparison chart

	WEP	WPA
Stands for	Wired Equivalent Privacy	Wi-Fi Protected Access
What is it?	A security protocol for wireless networks introduced in 1999 to provide data confidentiality comparable to a traditional wired network.	A security protocol developed by the Wi-Fi Alliance in 2003 for use in securing wireless networks; designed to replace the WEP protocol.
Methods	Through the use of a security algorithm for IEEE 802.11 wireless networks, it works to create a wireless network that is as secure as a wired network.	As a temporary solution to WEP's problems, WPA still uses WEP's insecure RC4 stream cipher but provides extra security through TKIP.
Uses	Wireless security through the use of an encryption key.	Wireless security through the use of a password.
Authentication method	Open system authentication or shared key authentication	Authentication through the use of a 64 digit hexadecimal key or an 8 to 63 character passcode.

- **Conclusion**

In this paper, a variety of methods of cryptography in wireless sensor network we examined and then to compare these methods we have to use this comparison to notice which way over other methods is the superiority of using this method, we can better and more robust security for wireless sensor networks, we provide and less about hackers attacks.

- **REFERENCES**

[1] A.K.M.M. Islam and K. Wada, "Communication Protocols on Dynamic Cluster - based Wireless Sensor Network," Informatics, Electronics & Vision (ICIEV), 2013 International Conf erence on. Dhaka, pp. 1-6, 2013.

[2] M. Borouomand zadeh, M. Hashemiand M. Mohmedi, "Target Tracking Techniques for Wireless Sensor Networks" International Research Journal of Applied and Basic Sciences, Vol. 5, No. 7, pp. 820-823, 2013.

[3] *IEEE ñ 802.11-1997 Information Technology-telecommunications And Information exchange Between Systems-Local And Metropolitan Area Networks-specific Requirements-part 11: Wireless Lan Medium Access Control (MAC) And Physical Layer (PHY) Specifications. 1997.*

[4] *http://security.itpro.ir/articles/15745/*

[5] *http://www.diffen.com/difference/WEP_vs_WPA*

[6] *http://searchsecurity.techtarget.com/WLAN-security-Best-practices-for-wireless-network-security*

https://sites.google.com/site/IJCSWN/
ISSN 2519-0814