Sjournals
Scientific Journals
Scientific Journal of Review (2015) 4(4) 55-70
ISSN 2322-2433
doi: 10.14196/sjr.v4i4.1840

Contents lists available at Sjournals
Scientific Journal of REVIEW
Journal homepage: www.Sjournals.com

Review article

The applications of wireless sensor networks in military environments

A.A. Baradaran
Department of computer science, Payame Noor University, Kashan,Islamic Republic of Iran.

*Corresponding author; Department of computer science, Payame Noor University, Kashan,Islamic Republic of Iran.

ARTICLE INFO

Article history,
Received 03 March 2015
Accepted 27 March 2015
Available online 28 April 2015

Keywords,
Wireless sensor networks
Military areas
Secure data
Data aggregation

ABSTRACT

Nowadays, I have to find methods and new weapons on the battlefield to enhance the military capability that the most important is increasing of power in electronic wars. Maybe in the past, many soldiers on the battlefield, commanded of strong of the commanders, increase the military strength of a country and use of new techniques on the battlefield, caused which we win but nowadays all of them have been affected by electronic wars. With the help of sensor networks on the battlefield, we can obtain much information on many war fronts. (For example, Battlefield simulation, enemy's front simulation, espionage, movement control and surveillance in the region, number of enemy soldiers). We can distribute smart dusts (like of mica particles) by planes or missiles. Then we can analyze all of information with the help of special software. In this research I have tried to explore the challenges involved in military environments. At the end to solve the existing problems, I have presented solutions with the help of wireless sensor networks.

1. Introduction

Wireless sensor networks are composed of a number of nodes that are distributed in the region in order to get the information and send it to the Base station (BS) [1, 2]. Mostly, diffusion of nodes in the

area is randomize and without human intervention. The nodes have little energy that this issue limits the lifetime of this kind of network. In recent years, researchers have been able to provide approaches. Then, somewhat with the help of these approaches, they have been able to improve the network lifetime. These techniques include: Routing, clustering, data aggregation, routing based on genetic, secure routing and clustering and etc [3]. The self-organization, fault tolerance and quick order in WSN, has caused that this type of network be one of the high useful methods in sensitive environments. On the battlefield we can use from WSNs for identification and check of the number of enemy troops and equipment, the path of enemy forces or Friendly forces and target tracking systems [4,5]. Figure 1 shows the structure of WSNs.

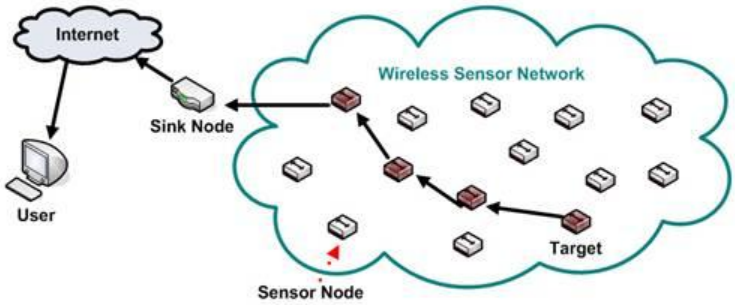

Fig. 1. Structure of WSN.

Usually, the received information in WSNs is sent to the BS by single-hop or multi-hop method [6, 7]. In the single-hop method, the collected information by nodes is sent to the BS directly. In the multi-hop method [45], after information storage in nodes, information sends to the high levels. Then high level nodes send information to the BS [8, 9]. Figure 2 shows the multi-hop method.

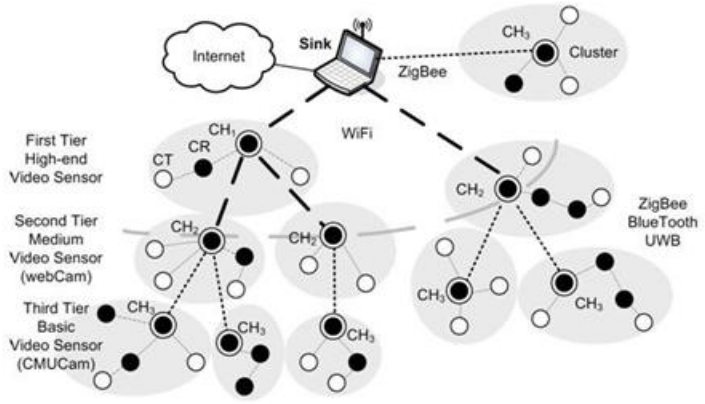

Fig. 2. Multi-tier Architecture of WWSNs (Wide Wireless Sensor Networks).

Often in the multi-hop method uses the clustering. In this method at first is done clustering. Then in each cluster selects the node with high fitness. This node is called cluster head (CH). Finally, Cluster heads sent them information to higher level cluster head or send to the BS. Figure 3 shows the clustering approach [10, 11 and 47].

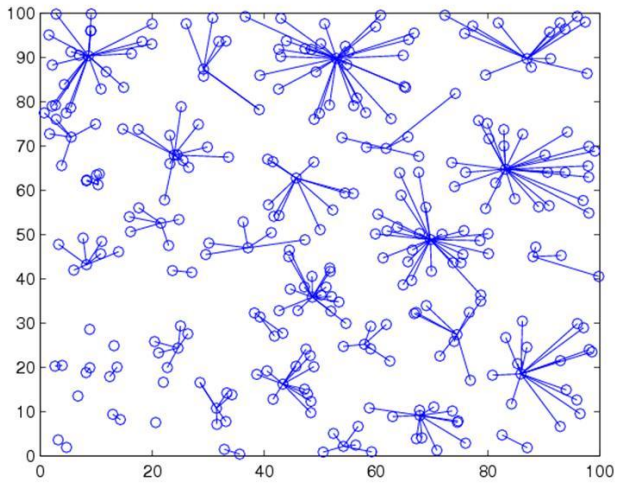

Fig. 3. Clustering in WSN.

Military applications of WSN

On the battlefield, we can use of WSNs for Things like creating Identify and survey of the equipment and enemy forces, movement of enemy forces and target tracking systems. Also wireless sensor networks can be used for tracing listed property and movement of militant groups in the battlefield [11, 12 and 13]. The overall, applications of WSN include:

- Control of the house temperature or office
- Concentrations of chemical materials
- Distribution of military commands
- Receiving logistic information
- Espionage information

Perhaps one of the reasons that limit the growth of this type of network in the military environments is lack of appropriate equipment. One of the key issues in the military region is information security. Equipment used in WSN must have the ability to retain information. The overall following cases can be effective on the equipment used in the military region [14, 15]:

- Resistance for the arrest
- Navigation
- Electronic warfare threats
- Development of Security

Military applications in a sensor network depend on the type of military operations and the type of sensor. Types of military operations are following cases [16, 17 and 18]:

- Operation is in town or on the battlefield.
- Operation is for peacekeeping or assistance.
- Operation is for Forces protection.

Military applications according to the type sensor are included:

- Operations in a particular area (for example, radar or meteorological)
- Photography
- Influence operations
- Tracking
- Frazzle
-

Table 1 shows the different categories of military applications of WSN due to the type of sensor.

Table 1
The military applications of WSN according to the type of sensor.

Sensor types	Operation scenario			
	Battlefield	Urban	OTW	Force protection
Presence / Intrusion	SHLM, AAP, ASW	SDT		SHLM, AAP, SDT
CBRNE	RCS		VDM	VDM, RCS
Ranging	ASW	EARS, INS	BL, INS	EARS, BL, SDL, PP
Imaging		SDL, MCM	MCM	SDL, MCM, PP
Noise		ATS	ATS	ATS

Network size

For most of operations in a military region that have been covered by sensors, it is better to be the network size between 5 to 20 square kilometers [19, 20]. Useful range of sensors is better to be between 250 and 500 meters that this needs to a network with low nodes. For example, in some smooth areas, that disorders are less, Communication ranges a kilometer is good.

Information flow

At the beginning of WSN in sensitive regions, one-way communication was appropriate. In military areas would be appropriate this method for communication between soldiers and commanders for situational information in the short term. For example, we can refer to the feature of navigation cameras. Initially, the cameras were able to communicate in a way. It means that these cameras had just been unable to send receive information. However, the need for two-way communication is essential. Two-way communication in military networks has the need for high security [21, 22].

Duration of the application

Some networks are able to perform operations on the day or at night. In some cases a network works more than a day (for example, a week or more). All of these problems depend on the type of node or nodes energy. Generally, following cases can affect on the lifetime of the network:

- Usage type
- Military region type - Flatness of the area
- The initial energy of sensors
- The distance between the sensor and the BS
- The transmission medium

Military intangible operations

For forces protection and information, it is better to be camouflaged nodes. One approach is to be covered nodes with electromagnetic coverage. This makes that the nodes remain hidden from enemy sight. For example, we can refer to camouflage in the mountainous areas that are covered with snow. The main reason that makes official forces camouflage themselves in snow is enemy modern sensors that they

can to identify and discover the forces in all weather conditions. Generally enemy sensors are located in areas of ultraviolet, visible, near infrared, thermal infrared and radar.

UV sensors are very important in snowy areas because snow reflects UV energy well but man-made objects do not reflect this energy [23, 24]. The winter color patterns, modern coatings suitable for snowy regions, are another of the main means of defense against this type of sensor. Coping methods with these sensors is modern white cover with reflection characteristics of snow. The use of each type of the smoke is causing loss of the sensors. Snowy building walls can also be effective. The night vision cameras or infrared sensors can identify the goals of mobile and stationary equipment. Thus the observance of discipline and prevent the spread of light and the use of appropriate camouflage clothing is effective. Thermal sensors at night and in conditions of snow, rain and dust are effective. Prevent heat radiation and heat-absorbing coating by camouflage nets can be effective. Radar sensors can easily detect the location of their forces. Usually radars range for finding people is 10 to 20 km. But they can't to discover targets that are behind barriers.

Data type

Type of data has an important influence on the use of WSN in the military. For example, limited amounts of text to report (less than 30 bytes), it can be done between the sender and receiver [25]. We should note that data transmission in military environments should be approved. As a solution, we can mention to the TCP / IP protocol. This protocol uses the approach, three-way handshake to establish a connection. In general, a high transmission rate is not important, but the important thing is that the data with each volume, to be transmitted securely. Perhaps if in the first step be resolved the security issue, has provided high security combined with high transfer rate spontaneously. This will increase the reliability of data.

The reliability of data

In some military applications just receive data is important (for example, such as Investigate the Situation of peace or ceasefire). This has need for the encoding different techniques [26, 27]. For example, it is better for us using the UDP protocol in environments that sending is important. The reliability of data means we can transfer data without any intervention and by a secure way.

Involvement and influence in the military environment

Collected data should not be placed available to other organizations or enemies (For example, in the military organization). Even this technique should be used when the nodes are captured by the enemy. In other words, the sensor network in the military should be able to detect enemy attack and able to react fast to be attacked. In general, following items control to ensure the security [28, 29 and 30]:

- Eavesdropping
- Spoofing
- Messaging Integration
- Rejecting network unknown messages
- Type of Geographic Area
- Secure routing protocol

Types of military regions

When using wireless sensor networks, we pay special attention to the region type. On the battlefields, the environment can be divided into the following two categories:

- Terrestrial areas (dry)
- Aqueous areas (submarine)

The terrestrial regions include mountainous areas, deserts, canyons and forests that most battles takes place in these regions. The aqueous regions are included Lakes, seas, oceans and underwater regions that the use of sensor networks in this environment is very difficult.

Techniques used by wireless sensor networks in military regions

With the help of sensor networks in the battlefield we can get a lot of battle fronts. We can use aircraft and missiles that contain smart particles (such as mica mote). Then we control them by special software [31, 32, 33 and 34].

The use of integrated data models in military regions

One of the most common methods is the use of sensorial integration data models for monitoring and environmental surveillance. Since this method uses a set of processing nodes and the management of its operations, therefore, to make we be able to transfer the information from the sensors to the processing centers, we must we must to choose an appropriate architecture. Select the appropriate architecture should be done intelligently and with respect to certain criteria and process parameters of the sensor. Thus, decisions about the choice of architecture depend on different conditions that are including the data integration operations, Selection criteria of architecture and targets conditions. The most common of these models is the JDL model (Joint Directors of Laboratories). The JDL is a multilevel process that is based on automatic detection, classification, association, data correlation, information from one or more source to refine the location, identity estimation, complete and timely assessments of situations and threats. These methods, estimates and obtained measurements analyzes continuously. Then, with continuous evaluation of the results, it provides a self-correcting process in order to improve results.

Overall, build this model can be done by a service-oriented architecture. Service oriented architecture is a structure where all services are created, deployed and managed. The main goal of service-oriented systems is increasing the ability of information systems to respond to area issues. The service - oriented architecture enables us to change the sensor data mixing system, quickly. System Integration capabilities and platforms are the most important issues that service-oriented architecture has attended to it that with this feature we can easily integrate several sensorial information integration platform if necessary.

Methods based on secure data aggregation and service oriented architecture

In the data aggregation, we try to measured values in the real world be related to a specific purpose. Also should be recognized that obtained values are related to which goal. In distributed systems, because the required data to track are obtained the different processing nodes should be compared to provide an accurate design of the object to tracking. The nearest neighbor algorithms, data aggregation with joint possibility (JPDA), Lagrange discount, intelligent neural networks and fuzzy logic are the main approaches that have been proposed for data aggregation. Figure 4 shows the result this approach.

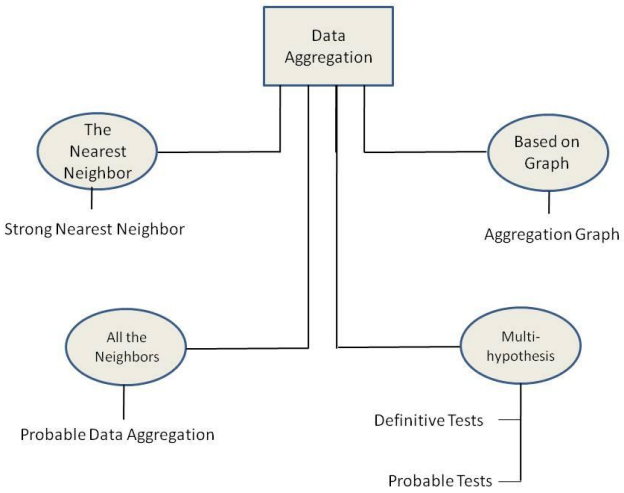

Fig. 4. Algorithms for objectives data aggregation.

State estimation algorithms in the military environment

State estimation is a process based on the obtained measurements that calculates the target position. For example, the target motion analysis is done by an active tracer that only determines target behavior (such as range of motion and speed) and they don't care for the distance. Algorithms such as Kalman filters, multi-level resolution filters, multi-model algorithms, minor filters and artificial intelligence approaches are the main approaches that are used for estimating the status of the targets.

Target identification algorithms

Objects are identified in the category stage. Usually it is assumed that the local terminals, from their sensory data that have enough confidence in their values are used for the best estimate of their identity and purpose. After a national recognition, obtained data is sent to other nodes. Then, according to other terminals data, we get an accurate overall design. In other words, the identification stage, task of object classification, estimation of target features based on local data and transferring the data to the external system is responsible for the overall problem. The Bayesian inference algorithms, Dumpster - Schaffer composition rules, artificial intelligent networks, expert systems, voting approaches and distributed classification are approaches that are used for identification of purposes. In Figure 5, possible algorithms are shown for identification of purposes separately. As can be seen, for production processes for data consistency and data aggregation, state estimation and identification, are different algorithms. Also, after that process the data consistency, data aggregation, state estimation and identification becomes as services then we can to produce the new services that able to use of these services. These new services include: Size analysis services and objectives. This service determines whether the environment has been traced the goals searching or not and if are tracking, how much is measuring goals. Target analyzes service to determine how many targets there are in the environment monitoring. The type of target analyzes service to determine that what is the kind of targets and motion analysis service to determine that they where are located.

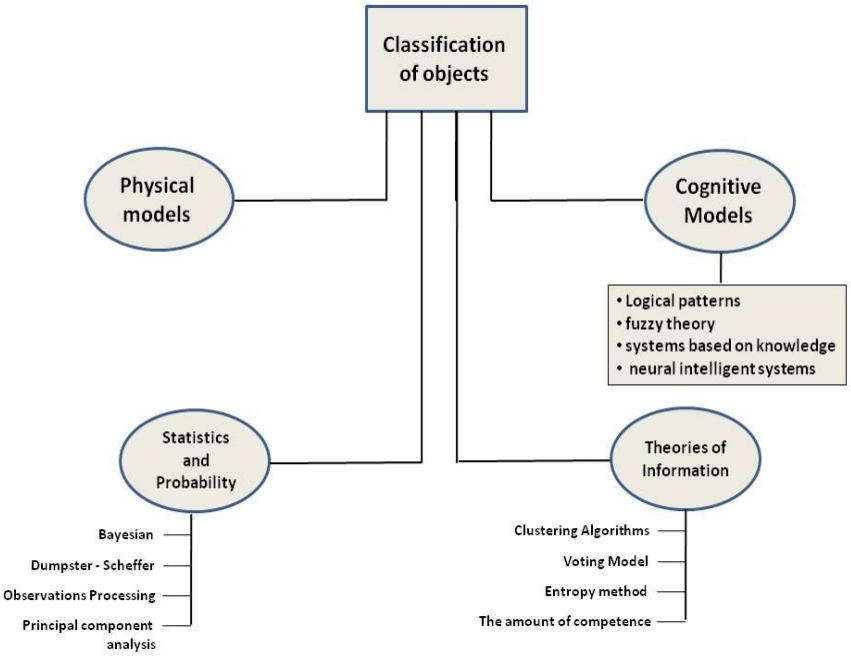

Fig. 5. Possible algorithms for identification of target.

Intelligent algorithms to determine the position in the military environment

One of the problems of sensor networks is many errors in the nodes estimation. This problem in critical applications such as military environment is problematic. Because percent of low error, it provides a great risk. One of the methods is presented in this field is TABU method. This method is based on the Meta Heuristic search process. This method is a dynamic neighborhood search technique that during the search is not affected the local minimum. The main feature of this method is that points of search in the previous steps, in the next steps are not abandoned and are stored in memory. In this method search can be done by an objective function (such as genetic algorithms).

The other method in this field is Marzullo algorithm. This method is included: Prepare a table of sources, sorting, and then search (efficient search) for distance participation.

Types of military attack in WSN

Generally, major attacks in wireless sensor networks are active and passive attacks. In the passive attacks, hostile nodes will not eliminate the operations of routing protocols. The main purpose this type of attack is to obtain a set of valuable information. Also in this type of attack, hostile node to save on own energy consumption refuses to cooperate to provide services to other network nodes. Often hostile nodes to perform passive attacks do not use much power. Detect these types of attacks in wireless sensor networks is very difficult. Passive attacks, including: Eavesdropping, Location disclosure attack and Selfishness of nodes. The active attack is an attack that in which a hostile node tries by energy consumption and power, achieved confidential information. Although to detect active attacks against passive attacks easier, but they are the threat of severe on the network nodes. The active attacks are included: Deformation-Based Attacks, Redirection to the serial number changes, Redirect by the number of steps, Prevention of service via source redirect, impersonation attack, rushing attack, black hole attack, gray hole attack, neighbors attack, jellyfish attack, denial of service attack, worm hole attack and Jamming attack[35,36,38,39 and 40].

Guarantee the security methods in WSN

Ariadne protocol

This protocol is used to prevent attacks and is resistant in front of security vulnerabilities. This protocol instead of using public key uses symmetric encryption. Also for authentication of the message, are used for an authentication, message that this message creates by a hashed code.

Dsdv protocol (dynamic destination sequenced distance-vector routing protocol)

The DSDV algorithm is based on the number of destinations. This algorithm is a step by step routing protocol that uses the mechanism of developed Bellman – Ford. In this method, each node distributes updates of the path generally. Each node keeps a routing table that is included: destination, the number of steps to reach the destination sequence number corresponds to the destination node. The sequence number is used to specify the old paths. In fact, each path sequence number that is larger than the destination, is a new route that this is used to avoid the loops. That's always are used paths that have larger sequence number. Figure 6 shows the DSDV protocol.

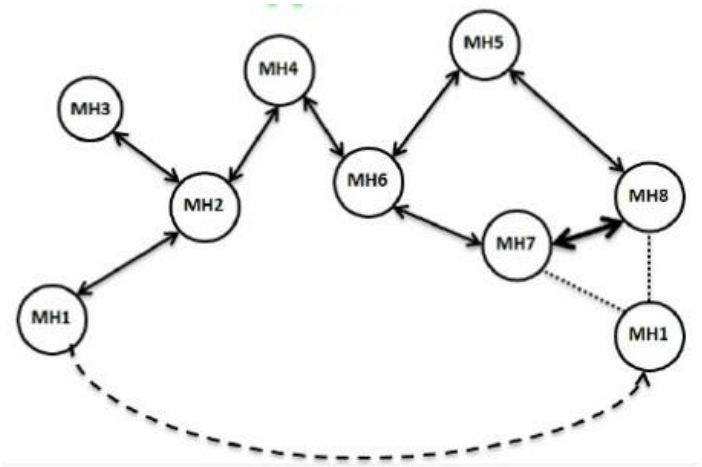

Fig. 6. The DSDV Method.

Saodv protocol

This protocol is based on Public Key Cryptography. The SAODV routing messages include: Route request messages, Route response and route errors. These messages use digital signatures to ensure the integrity and accuracy of credit. Then node, receives the message of signed routing. Finally, the nodes receiving the message are confirmed by using the public key of a digital signature.

ARAN protocol

This protocol is called route identification protocol. This algorithm is based on the AODV algorithm. The protocol using cryptographic mechanisms such as authentication, message integrity and non-repudiation, is considered security. This protocol uses asymmetric key encryption and is consisting of three steps:

- Create an initial certificate
- Route discovery
- Find the shortest path

This protocol by using a public encryption and a certificate attempts to discover a route and find the optimal route. Also by using the timestamp prevents spoofing attacks and repeated broadcasting attacks. Compared with other routing protocols this protocol is simple and non-secure.

SRP protocol

This protocol is for to deal with attacks that have been discontinued route discovery process. This protocol ensures correct identification topology information. Also the SRP algorithm can to discover all possible routes between two nodes. In addition to these two nodes two nodes have a common key to communicate and confirm. The main idea of the SRP is setting the security relationship between source and destination nodes, without requiring secure data encryption communication through intermediary nodes. This algorithm is suitable for military environments and sensitive regions.

SEAD protocol

Secure efficient distance vector routing protocol (SEAD) is a pro-active routing protocol based on the DSDV. In This method, nodes hold the interval data and the next node to the destination in their own. In this protocol there is a routing table in each node that they contain a list of all the possible routes. In every part of the table there are the destination address and the nearest distance between the node and neighboring nodes (metric). Each node for update own table, Each node updates your table, every so often sends a request message to its neighbors in order to make route for new ways to save on your table.

SPAAR protocol

This protocol acts by using location information to enhance network security and performance. As long as the information about the position of nodes is kept, the network is aware of the existence of unauthorized nodes. Table 2 shows a comparison of various protocols.

Table 2
Comparisons between protocols.

Security Technique	Secured Multicast Protocol	Basic Security Technique	Design Consideration	Topology Changes Adaptation	Scability	Packet overhead	Processing
ARAN	MAODV	Asymmetric cryptography key and certificate server	Based on AODV, and designed to secure Reactive routing protocol	Good adaptation	Average scability	Average overhead	High processing
SRP	ODMRP	Digital signature and hash chain function	Security extension for Reactive routing protocols	Average adaptation	Average scability	Average overhead	Low processing
SEAD	MZRP, MAODV	Hash chain function	Security extension to DSDV protocols	Good adaptation	Average scability	High overhead	Average processing
ARIDANE	AMRIS	Symmetric cryptography key and hash chain function	Based on the basic operations of DSR protocol	Average adaptation	Average scability	Low overhead	Average processing
SAODV	MAODV	Asymmetric cryptography key, Digital signature and hash chain function	Designed to be an security extension for AODV	Average adaptation	Average scability	Average overhead	High processing

SAR protocol

This protocol is based on a Trust-Based Framework. Every node in the network is assigned a trust level. After the attacks in this framework, we can again review level of trust and authenticity of the message. To follow a hierarchical structure based on trust; this method is used secret sharing techniques such as encryption, public key, and shared key.

New approaches to security in military environments based on WSN

Key management

The main task of key management is allowing access to authorized users. This occurs when those users can to have access using dedicated keys [41, 42 and 43]. Key management includes a set of tricks and ways to establish and maintain communication between the authorized both sides of the communication. Communication key is a situation that both parties communicate share certain data that are needed for encoding algorithms. Key-based methods should be able to provide a proper key for the sharing between individuals.

Safe routes

The basis of this idea is that the attacker cannot listen to all of the paths between the source node and the destination and hears them all. In this process can be implemented the secure data aggregation techniques, or methods based on public key encoding. The main goal of this approach is finding the best route along with security.

Approaches based on malicious node identify

A malicious node may be social or personal misconduct. In the individual misconduct, a single node provides attempting to abuse in the routing operation, but in the social individual, number of nodes together does it. Often is difficult detect and prevent acts of mass malicious. A node cannot send a package to particular causes. Also set of nodes can do it. These two cases are good examples of misconduct, individually and collectively. One of these techniques is the watchdog. This technique is often used with path rater. This technique has collision problem.

Path rater to select a route, instead selection of the shortest route, uses a simple rating algorithm. Path rater runs by all nodes in the network. This method has problems such as:

- Lack of flexibility
- Behavioral
- New Node Anonymity
- Re-entry of malicious node
- Encouraging Selfishness and Greed

Proposed methods to enhance the security of military networks based on WSN

The proposed techniques for dealing with eavesdropping

Greater use of hiding and encrypting communications and code information and the control method In the series of meetings and common codes such as cookies or effective use of information hiding techniques.

Improvement of TCP / IP protocol

This protocol has the ability of discriminatory of a program on a computer with other programs. This protocol after receiving data from a program sends them to the application on the target machine. The statutory sessions of TCP / IP, ends by sending a TCP reset packet from one of the parties. An attacker

within the network can forge the sender's address on the package before the deadline. Also, they can be disrupted or destroyed part of the transaction. An attacker may be able to steal the whole network information. Defending against network-level attacks through application is very difficult, but hiding can be effective.

Secure routing

A good routing algorithm in the network must be able to build a path to the right and to keep it. This means that not to allow that hostile nodes prevent the construction or maintenance of the correct path. In general an algorithm is secure if the following conditions exist:

- Routing signals not be falsified.
- Manipulated signals cannot be injected into the network.
- Routing messages during transmission not changed.
- Routing loops are not created during the activities of the enemy.
- Shortest path not changed by hostile nodes.
- Non-authorized nodes should be excluded from the network.

Secure location for the node

The position of each node in the network to critical applications such as sensitive monitor and caring battlefield is very significant and important. In the discussion the position of the nodes, we must pay attention to three factors:

- Energy efficient
- Correctness or accuracy (precision)
- Security

Positioning techniques can be done in three techniques:

- Triangulation technique
- Lateration technique
- Ultilateration technique

Figure 7 shows the three techniques.

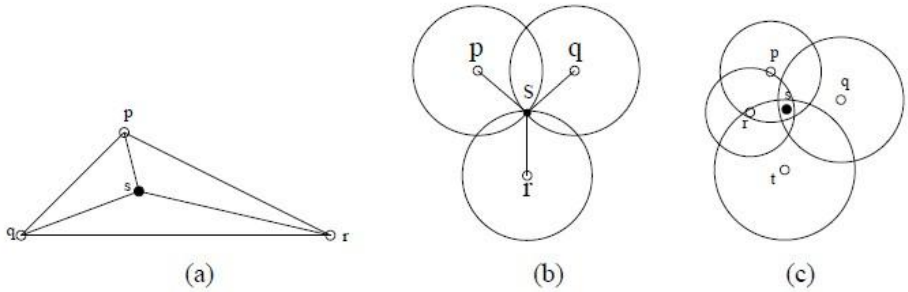

Fig. 7. Triangulation (a), Lateration (b) and Ultilateration (c) techniques.

These three methods have complex mathematical calculations that depending on the circumstances can be useful one of them. For example, the use of these methods is fit in polygons wireless sensor networks [48, 50].

Models based on the node trust

In this method, nodes use for calculate of rely on each other, from the direct and indirect trust. Each node keeps just its neighbors' trust values and they do not know about the number of network nodes. This makes are scalable the proposed method. The reliable systems are useful methods for detecting

deception or threats. These systems do their task by identify and eliminate malicious nodes in the network.

Security in separate levels of the network structure

In wide wireless sensor networks (WWSNs), sensor nodes are distributed in a large area. Because the energy of nodes is low, each node by itself is not able to send their data directly to the BS. Therefore, the network is divided into sections called clusters, where each cluster collects local node information and then sends to the BS in two ways:

- Single-hop method
- Multi-hop method

Security is important in both methods. Because if one node to be destroyed (especially a node that is as a vital node) may have wiped out the entire network information. Figure 8 shows the structure of a critical node in the network.

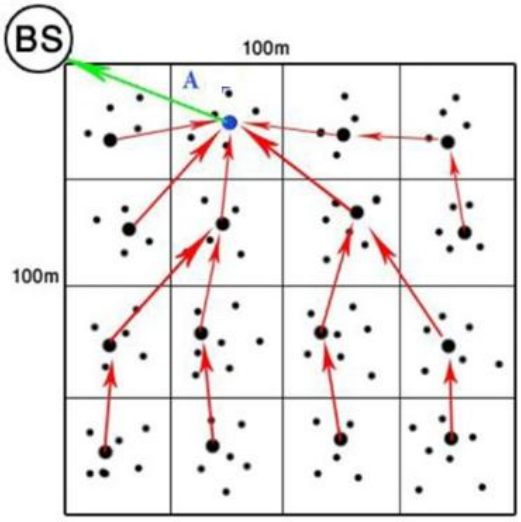

Fig. 8. Wireless sensor networks with vital node.

In Figure 7, the A-node is a critical node. If information this node is altered destroys the whole network information. The best approach is establishing the security node separately. Another method is that we establish a cluster-level security. This method requires efficient clustering algorithms that this method has a high cost. However, in sensitive environments such as military environment, may cost does not matter against data loss. However, both ideas require an intelligent way, considering the cost and security.

Conclusion

In this study, we tried to study WSN applications in sensitive environments, particularly in military regions. Issues such as security of data aggregation, the appropriate route, influence and interference in the network and eavesdropping are important in a military environment based on WSN. In this paper we have introduced types of military regions and their equipment. Then new approaches of WSN were presented in a military area. We evaluated issues such as target identification, target estimates, quality of service, moving targets and the technique of integration and mica particles. Also were introduced Types of attacks in sensor networks (active and non-active attacks). Then the solutions to deal with these attacks, we have presented. Our main objective in this study was that immediately after the introduction of the protocol, to consider how to deal with the security issues. In this regard, has been verified issues such as routing problems, message integrity, preserving packaging, security, message independence and

protocol attacks and how to deal with the attacks. We showed that the ways to deal with the attacks presented are acceptable in terms of performance, but each of them has strengths and weaknesses. Finally, we have presented new ideas based on the proposed methods. Some ideas were presented such as secure protocols, secure routing, secure node positions, routing based on trust and design factors. However, all these methods are needed to consider parameters such as cost, security, energy consumption and runtime. However, this idea can be a good approach at the current time.

References

1. Nallusamy, R., Duraiswamy, K., 2011. Solar Powered Wireless Sensor Networks for Environments Applications with Energy Efficient Routing Concepts. Informat. Technol. J., volume 10,pages:1-10
2. Ritu, S., Yogesh, C., Yudhvir, S., 2010. Analysis of Security Protocols in Wireless Sensor Network. Int. J. Adv. Network. Applicat., Volume 2, Pages: 707-713.
3. Michael, W., Klaus-Dieter, T., Kester, H., Graeme, B., 2008. Theoretical and practical aspects of military wireless sensor networks. J. Telecommunicat.Informat. Technol.
4. Walid, B., Yacine, C., Abdelmajid, B., 2013. A new class of Hash-Chain based key pre-distribution schemes for WSN. Comput. Communicat., Volume 38, pages:243-255.
5. Meenakshi, T., Gaur, M.S., Laxmi, V., Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN. The 8th International Symposium on Intelligent Systems Techniques for Ad Hoc and Wireless Sensor Networks (IST-AWSN), pages: 1101 – 1107, 2013
6. Hailun, T., Diethelm, O., John, Z., Sanjay, J., A confidential and DoS-resistant multi-hop code dissemination protocol for wireless sensor networks. Comput. Secur., Volume 32, Pages:36-55, 2013
7. Jia-qi, X.U., Lei, W., Can, M., Lei, S., Study of impacts of duty-cycle on overlapping multi-hop clustering in wireless sensor networks. J. China Uni. Posts Telecommunicat., Volume 19, 2012.
8. Dong-Kyu, L., Tae-Hyon, K., Seol, Y.J., Soon-Ju, K., 2011. A three-tier middleware architecture supporting bidirectional location tracking of numerous mobile nodes under legacy WSN environment. J. System. Arch., Volume 57,
9. Li, L., Yuan-an, L., Bi-hua, T., SNMS: an intelligent transportation system network architecture based on WSN and P2P network. J. China Uni. Posts Telecommunicat., Volume 14, 2007
10. Song, M.A.O., Cheng-lin, Z.H.A.O., Unequal clustering algorithm for WSN based on fuzzy logic and improved ACO. J. China Uni. Posts Telecommunicat., Volume 10, 2011
11. Mustapha, R.S., Abdelhamid, M., Hadj, S., Amar, A., 2012. Performance evaluation of network lifetime spatial-temporal distribution for WSN routing protocols. J. Net. Comput. Applicat., Volume 35,
12. Stefan, K., Stafrace, N.A., 2010. Military tactics in agent-based sinkhole attack detection for wireless ad hoc networks. Comput. Communicat., Volume 33.
13. Zhang, R., Li, D., Huang, H.F., Wang, Y., Wang, Y.Z., Xia, L.Z., Logistics Transportation Vehicle System for Information Acquisition Based on Wireless Sensor Network. Proc. Eng., Volume 29, 2012
14. Jiafu, W., Hui, S., Hehua, Y., Jianqi, L., 2011. A General Test Platform for Cyber-Physical Systems: Unmanned Vehicle with Wireless Sensor Network Navigation. Proc. Eng., Volume 24.
15. Younis, O., Fahmy, S., 2004. HEED: A hybrid energy-efficient distributed clustering approach for ad hocsensor networks. IEEE Trans. on Mobile Comput., 3(4), 660-669.
16. Devesh, P.S., Goudar, R.H., Mohammad, W., 2013., Hiding the Sink Location from the Passive Attack in WSN. Proc. Eng., Volume 64.
17. Huan, D., Zhao-min, Z., Xiao-Feng, G., 2013. Multi-target indoor localization and tracking on video monitoring system in a wireless sensor network. J. Net. Comput. Applicat., Volume 36.
18. Qiuhua, W., Huifang, C., Lei, X., Kuang, W., 2013. One-way hash chain-based self-healing group key distribution scheme with collusion resistance capability in wireless sensor networks. Ad. Hoc. Networks, Volume 11.
19. Nils, H., Ole, B., Steffen, P., 2011. An Automated System for an Analog Light-Sensor with Adjustable Measuring Range and High Resolution in WSN. Proc. Eng., Volume 25.

20. Vougioukas, S., Anastassiu, H.T., Regen, C., Zude, M., An energy Influence of foliage on radio path losses (PLs) for wireless sensor network (WSN) planning in orchards. Biosyst. Eng., Volume 114, 2013
21. Jiliang, Z., Qiying, C., Caixia, L., Runcai, H., 2010. A genetic algorithm based on extended sequence and topology encoding for the multicast protocol in two-tiered WSN. Expert System. with Applicat., Volume 37.
22. Ananth, V.K., 2010. Nikhil Singhal, Steven Weber, "Broadcast capacity of a WSN under communication and information coordination. Ad Hoc Networks, Volume 8.
23. Kelly, D.C., Dimmock, N.J., 1974. Fowl plague virus replication in mammalian cell-avian erythrocyte heterokaryons: Studies concerning the actinomycin D and ultra-violet light sensitive phase in influenza virus replication. Virol., Volume 61.
24. Shah, H.A., Mahdi, H.Y., Joji, M.O., 2011. Heat-shock-induced color-pattern changes of the blue pansy butterfly Junonia orithya: Physiological and evolutionary implications. J. Therm. Biol., Volume 36,
25. Abu, R.M., Kamal, M.d., Abdul, H., 2013. Reliable data approximation in wireless sensor network. Ad Hoc Networks, Volume 11.
26. Jing, W., Liu, Y., 2012. Routing Protocol Based on Link Reliability for WSN. Phys. Proc., Volume 33.
27. Saamaja, V., Kiran, K., Rachuri, C., Siva, R.M., 2010. Using mobile data collectors to improve network lifetime of wireless sensor networks with reliability constraints. J. Parall. Distr. Comput., Volume 70.
28. Zoran, B., Veljko, M., 2013. Chapter 2 - Novel System Architectures for Semantic-Based Integration of Sensor Networks. Adv. Comput., Volume 90.
29. Petr, K., Jiri, K., Radim, S., Vojtech, L., 2013. Prototyping the visualization of geographic and sensor data for agric. Comput. Electron. Agric., Volume 97.
30. Tae-Hong, S., Sangyoon, C., Su-Won, Y., Soon-Wook, K., 2011. A service-oriented integrated information framework for RFID/WSN-based intelligent construction supply chain management. Automat. Construct., Volume 20.
31. Miloud, B., Yacine, C., 2011. Abdelraouf Ouadjaout, Noureddine Lasla, Nadjib Badache, " Efficient data aggregation with in-network integrity control for WSN. J. Parall. Distr. Comput., Volume 72.
32. Sabrina, S., Luigi, A.G., Gennaro, B., 2012. Alberto Coen-Porisini. DyDAP: A dynamic data aggregation scheme for privacy aware wireless sensor networks. J. System. Softw., Volume 85.
33. Pourpeighambar, S.B., Sabaei, M., 2013. Spatial correlation aware protocols for efficient data aggregation of moving object in wireless sensor networks. Sci. Iran., Volume 20.
34. Licheng, W., Lihua, W., Yun, P., Zonghua, Z., Yixian, Y., 2011. Discrete logarithm based additively homomorphic encryption and secure data aggregation. Inform. Sci., Volume 181.
35. Meenakshi, T., Gaur, M.S., Laxmi, V., 2013. Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN. Proc. Comput. Sci., Volume 19,
36. Kiran, K.P., Shivani, S., 2013. Protocol for Latency Reduction of Prioritized Traffic in WSN. Proc. Comput. Sci., Volume 19.
37. Meenakshi, T., Gaur, M.S., Laxmi, V., 2013. Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN. Proc. Comput. Sci., Volume 19.
38. Miloud, B., Yacine, C., Abdelraouf, O., Noureddine, L., Nadjib, B., 2012. Efficient data aggregation with in-network integrity control for WSN. J. Parall. Distr. Comput., Volume 72.
39. Wen, T.Z., Jianying, Z., Robert, H., Deng, F.B., 2012. Detecting node replication attacks in wireless sensor networks: A survey. J. Net. Comput. Appl., Volume 35.
40. Annlin, S.V., Jeba, B., 2013. Paramasivan, Energy efficient multipath data transfer scheme to mitigate false data injection attack in wireless sensor networks. Comput. Electr. Eng., Volume 39.
41. Ozgur, K.S., 2013. Large scale wireless sensor networks with multi-level dynamic key management scheme. J. System. Arch., Volume 59.
42. Rodrigo, R., Cristina, A., Javier, L., Nicolas, S., 2011. Key management systems for sensor networks in the context of the Internet of Things.Comput. Electr. Eng., Volume 37,
43. Michael, C., Jung-Min, P., Mohamed, E., 2007. Key management for long-lived sensor networks in hostile environments. Comput. Communicat., Volume 30.

44. Amir, A.B., Arash, G.D., javad, A., 2011. RGWSN: Presenting a genetic-based routing algorithm to reduce energy consumption in wireless sensor network. IJCSI Internat. J. Comput. Sci. Issu., Vol. 8, Issue 5, September.
45. Amir, A.Ba., Arash, G.D., 2012. CRCWSN: Presenting a Routing Algorithm by Using Re-clustering to Reduce Energy Consumption in Wireless Sensor Networks. Internat. J. Comput. Communications control Agora Univ., Romania.
46. Amir, A.Ba., Arash, G.D., Abootorab, A., 2012. KGAWSN: An Effective Way to Reduce Energy Consumption in Wireless Sensor Networks by K-means and Genetic Algorithms. Internat. J. Comput. Applic., (0975 – 888) Volume 48– No.12, June USA
47. Elham, R., Amir, A.B., Atefeh, H., 2013. TDTCGE: Two Dimensional Technique Based On Center of Gravity and Energy Center in Wireless Sensor Network", J. Basic. Appl. Sci. Res., 3(8)194-201.
48. Amir, A.B., Hassan, H., Hamed, Q., Mehrdad, H., 2013. Reviewing the New Methods of Routing for the Reduction of Energy Consumption in Wireless Sensor Network", J. Basic. Appl. Sci. Res., 3(8)194- 201.
49. Atefeh, H., Amir, A.B., Elham, R., 2013. IMKREC: Improved k-means Algorithm Method for Reducing Energy Consumption in Wireless Sensor Networks ", J. Basic. Appl. Sci. Res., 3(9)77- 88.
50. Amir, A.B., 2013. RAWSN: A Routing Algorithm Based on Auxiliary Nodes to Reduce Energy Consumption in Wireless Sensor Networks. J. Sci. Islam. Republ. Iran., 24(4): 355 – 359.