УДК 004.056: 004.73

Е.С. Абрамов, Е.С. Басан, Виджай Лакшми

РАЗРАБОТКА ЗАЩИЩЕННОГО ПРОТОКОЛА УПРАВЛЕНИЯ МОБИЛЬНОЙ КЛАСТЕРНОЙ СЕНСОРНОЙ СЕТЬЮ

Обеспечение защиты беспроводной сенсорной сети, топология которой динамически изменяется за счет постоянного перемещения узлов сети является нетривиальной задачей. Для такой сети необходимо разрабатывать собственные методы и протоколы защиты, которые обеспечили бы безопасную, эффективную и максимально продолжительную работу сети. Предлагается защищенный протокол управления мобильной кластерной сенсорной сетью. Применение кластеризации сети позволяет разбить сети на отдельные группы сенсоров, которые контролируются главой кластера (ГК), тем самым уменьшить нагрузку на базовую станцию (БС), увеличить пропускную способность сети и продлить продолжительность жизни узлов, а также обеспечить дополнительный контроль за каждым узлом сети. Использование системы управления доверием узлов позволяет выстраивать доверенные соединения между узлами сети и предотвращать нежелательные действия злоумышленника. Данная система обеспечивает защиту от внутреннего злоумышленника, при внедрении атакующего под видом законного пользователя в сеть, а также при перехвате узла сети.

Беспроводные сенсорные сети; кластеризация; атаки; доверие; протокол; алгоритмы; обнаружение аномалий; подлинность; оценка уровня доверия.

E.S. Abramov, E.S. Basan, Vijay Laxmi

DEVELOPMENT OF SECURE PROTOCOL FOR MOBILE CLUSTER SENSOR NETWORK MANAGMENT

Ensuring the protection of wireless sensor network with topology changes dynamically due to the constant movement of nodes is not a trivial task. For such a network, you need to develop your own methods and security protocols that would ensure safe, effective and maximum network uptime. This paper proposes secure control protocol for mobile clustering wireless sensor network. Application of clustering allows to split the network into separate groups of sensors that can be monitored by the cluster head (CH), thereby to reduce the load on the base station (BS), to increase network capacity and to extend the lifespan of nodes, as well as provide additional control for each network node. Using the confidence level control system allows to build trusted connections between network nodes and prevent malicious actions of the attacker. This system provides protection against malicious insiders, against the introduction of the attacker into the guise of a legitimate user to the network, as well as against the interception of network node.

Wireless sensor networks; clustering; attack; trust; protocol; algorithms; anomaly detection; authenticity; confidence level.

Introduction. The main purpose of this paper is to provide a protocol that could protect mobile sensor networks of all major types of attacks, while not significantly reducing the power consumption of nodes and their life expectancy network. In the proposed protocol such security mechanisms and algorithms were implemented :

- Algorithm for determining the confidence level in the network node;
- Protocol initialization Algorithm;
- Cluster-head pre-selection algorithm ;
- Algorithm of network's secure partition into clusters;
- Node migration algorithm.

Secure operation of these algorithms is based on the use of trust management in wireless sensor network (WSN).The system is based on the collection and exchange of data between adjacent nodes and calculating of the values of a confidence on the basis of the feature sets. This system will cope with the threats posed by malicious insiders and with the threat of compromised node. It will detect and isolate abnormal node.

To provide protection against external attacker one must use nodes authentication.WSN nodes features are limited energy and computational resources. Regarding this, to ensure that the duration of the WSN, as well as to reduce the load on the nodes' computing power it is necessary to use approaches of lightweight cryptography for authentication process. In this paper there is an overview of authentication algorithm, the detailed development of the algorithm is planned for the further work.

Thus, taking into account the architectural features of WSN the following features should be considered:

- ♦ Since there are mobile nodes, the clustering process should take into account the changes in the network topology. Therefore, the process should not be loaded by complex calculations with using bulk algorithms, otherwise the WSN will not cope with the job.
- ♦ Cluster head is not a constant role, as its resources can be significantly reduced and the replacement he can come to another node.
- ♦ One node may migrate from the cluster to the cluster and thus it is necessary to have assurance that it is a trusted node, each time it joins the new cluster.

1. Previous research. In most existing clustering algorithms, the nodes themselves decide how they should be grouped together and basically it depends on the position of the head of the cluster. Also most techniques involve the use of secret keys as in [1] and [2].Thus for each group of nodes, or for different purposes different keys are used. This approach is possible to protect against an external attacker, but does not guarantee protection against malicious insiders, which holds keys or from malicious node interception.

In [3] the protected circuit cluster formation in wireless sensor networks is described. In this scheme, a pre-selection of the cluster head (CH) is based on determining of the node with the lowest ID. When connecting nodes to the cluster, both sides exchanges messages signed with a secret key . The authors of this article show many different situations in which the work of the proposed scheme is broken, and offer solutions to these situations. But this scheme does not consider the possibility of moving nodes.

In [4] the author proposes an energy-efficient homogeneous clustering algorithm. This algorithm is based on the fact that the base station preliminarily splits nodes into clusters according to their geo-location, and then cluster head selected randomly. The new head of the cluster must meet the following requirements: the node is not a cluster head in the previous cycle; the ratio of the current residual energy to the initial energy level should be as close to 1 as possible; most preferred the head of the cluster is the one that close to the acting head of the cluster. This method of partitioning into clusters is the most simple, energy-efficient and fast. But on the other hand there are absolutely no security mechanisms.

The author [5] proposes a protocol of a secured partition into clusters. This protocol is based on the exchange of messages between adjacent nodes and calculating of the value of a local maximum of each node of the cluster. At each stage of the protocol work, nodes exchange value of the local maximum cluster with its neighbors, and adjust its own values within the meaning neighbors. At the last stage, each node checks for compliance. If it detects intruder node among its neighbors, it removes it from the network and starts execution of the protocol from the first step. Otherwise, it produces a matching of values and continues its work.

2. Defining metrics for cluster head selection. In [6] the problem of choosing the head of the cluster and the secure wireless sensor network model was considered. The formula and parameters for the calculation of the level of node confidence value and the level of the node residual energy were given. So here we show only the final formulas for calculating the node confidence level (1) and the level of residual energy unit (2).

$$DT^{A,B} = \sum_{i=1}^{k} W_i * T_i^{A,B}, \tag{1}$$

$$Q_i^k(E) = Q_{k-1} - k*E_i. \tag{2}$$

In our work we also will add an extra node metric - mobility. When selecting a cluster head, the level of node mobility must be considered, as the lesser node agile, the longer it holds the cluster head role. The metric "relative mobility" $M_Y^{rel}(X)$ of node Y concerning the node X is calculated by the formula (3):

$$\mathrm{M_Y^{rel}(X)} = 10\log_{10}\frac{\mathrm{Pr_{X\to Y}^{new}}}{\mathrm{Pr_{X\to Y}^{old}}}. \tag{3}$$

We assume that the transmission power P_{tx}, the path loss model (or path attenuation model) and path loss coefficient (α) are known. It is possible to estimate the distance between sender and receiver, using the received signal's power P_{rx}, as proposed in [7]:

$$P_{rx} = c \times \frac{P_{tx}}{d^{\alpha}}, \tag{4}$$

$$d = \sqrt[\alpha]{c \times \frac{P_{tx}}{P_{rx}}}. \tag{5}$$

where *c* is a coefficient dependent on the path loss model. In free space, the received power is inversely proportional to the square of the distance between sender and receiver ($\alpha = 2$). Now calculate the total value of mobility on any node Y by calculating the variance (relative to zero) of the entire set of relative mobility values $\mathrm{M_Y^{rel}(X_i)}$, where X_i is a neighbor of Y, as suggested in [8].

$$\mathrm{M_Y} = \mathrm{D_0}\left(\mathrm{M_Y^{rel}(X_1), M_Y^{rel}(X_2), \dots M_Y^{rel}(X_m)}\right) = \mathrm{M}\left[(\mathrm{M_Y^{rel}})^2\right]. \tag{6}$$

Here, D_0 denotes the dispersion relative to zero (and not the average value of the sample) and is equal to $M[(M_Y^{rel})^2]$, where M denotes the mathematical expectation. The basic meaning of calculating the variance of the relative mobility values relative to each neighbor is in that a low value M_Y indicates that the Y is less movable relatively to its neighbors. On the other hand, a high value of M_Y indicates that a node Y is more mobile relatively to adjacent nodes.

3. Work secure protocol control mobile sensor network cluster

3.1. The protocol initialization. Before talking about clustering in general, it is necessary to separate the process into several stages. The main emphasis should be done to ensure that the attack will be blocked or otherwise attack must be detected in a real time. According to the idea of creating a clustering protocol all nodes will send to each other a certain types of messages in a specific order, wherein if an attacker wants to make some destructive actions, it would be anomaly. In this protocol the the base station (BS) is an initiator and is responsible for its execution in the first cycle of the network work, further this responsibility will fall on the CH.

Protocol initialization

1. The base station sends an initialization message (MsI) to all network nodes.

2. All nodes (N) obtains MsI consequentially, and then sends a response message R-MsI to BS in the same manner, as defined by timeout. BS receives information about the node ID and checks the ratio of a serial numbers.

3. The final step in the initialization process is a message from the base station ACK-MsI. This message is sent to all nodes provisioned, while if the node has not received such a message, the BS found it suspicious or malicious. Such node would not participate in the network activity further and will be isolated.

4. Initialized nodes mark established connection as trusted. In turn, the BS also puts these nodes to the list of trusted nodes, and among these nodes the cluster head will be selected in the future.

Initialization procedure serves for two purposes. First, in order to establish a trusted connection between the base station and nodes. Secondly, it is assumed that the base station stores the preloaded list of trusted nodes that are in the network and compares the obtained data with its own dynamic list.

3.2. Confidence level control system. As it was previously mentioned, many algorithms involves calculating of the level of confidence to the node. The algorithm for determining the confidence level is the basis of network clustering, as well as the basis of the entire network functioning as a whole. In the article [9], we proposed an algorithm for determining the confidence level. In this particular article the algorithm has been finally modified.

Algorithm for determining the confidence level to the network node

1. Node collects data from neighboring nodes on the specified parameters.

2. Node calculates the confidence level according to equation (1).

3. Node calculates the residual amount of energy (2).

4. Node sends the obtained data to the BS and to the neighboring nodes (located at a distance of a single hop).

5. BS calculates the average amount of energy.

6. BS also monitors traffic and calculates the eigen values (steps 1-3 of this algorithm).

7. BS compares its own values with the values obtained from the nodes:

a) If everything is correct, then continue the algorithm.

b) If the values do not match, the node that sent the incorrect values becomes untrusted, then continue the algorithm.

8. BS sends the calculated values of nodes.

9. Node calculates the values of the energy and confidence level by the formula (3). After that node compares the level of residual energy with the congestion level of the node:

1) If a node has a maximum value of residual energy level, then it also has either the minimum or average number of sent packets (Total pack)

$$\begin{cases} \mathrm{Q_i^k(E)} = \mathrm{max}; \\ \mathrm{Total\ pack} = \mathrm{min, average}. \end{cases} \qquad (7)$$

2) If a node has an average value of the residual energy level Qik(E) = average, then it also has the minimum number of sent packets conjunction with the average or the threshold value of the residual energy

$$\begin{cases} \mathrm{Q_i^k(E)} = \mathrm{average}; \\ \mathrm{Total\ pack} = \mathrm{average, threshold}. \end{cases} \qquad (8)$$

3) If a node has a minimum value of residual energy Qik (E) = min, then it can match the values from minimum to maximum

$$\begin{cases} \mathrm{Q_i^k(E)} = \mathrm{max}; \\ \mathrm{min} < \mathrm{Total\ pack} < max. \end{cases} \qquad (9)$$

10. If the result of the comparison found that this condition is not satisfied, the node sends the data to the CH, which performs a deep inspection by analyzing the types of sent packets.

Manage_pack – control packets - this group includes beacon packets, protocol initialization packets, warning packets.

Route_pack – routing packets - here, RREP, RREQ, ACK packets.

Data_pack – data packets – any packets in which information is transmitted with measurable indicators, ie notifications.

Thus, in case of most of the sent packets were from first and second groups, the node considered to be untrusted, and in case of the last group, node considered to be suspicious.

11. In case of identifying the untrusted or suspicious node, CH sends messages to all sensor-nodes in the cluster and to all neighboring CH.

3.3. Network clustering. The main feature of the proposed clustering algorithm is that nodes select the CH and the method of clustering based on the preliminary choice made by the BS, but not by themselves. This is necessary in order to:

- ♦ An attacker can affect the results of choosing the CH by intercepting values of sensor-nodes and fake them.
- ♦ An attacker can send the resulting value (result of the CH choice) with low signal power, so that some nodes will not receive it. As a result those nodes which do not receive the value have different value from the other receivers. Thus, these nodes can choose another node as the CH.

The algorithm of the pre-selection of the cluster head

1. BS announces the start of the CH selection process and sends a special message ECH-Msg to each node.

Note: This message carries the information for nodes that they have to calculate indicators of residual energy level, confidence level and the total value of mobility. In the reply message the base station will wait just for these indicators.

2. Sensors nodes perform steps 1-4 algorithm for determining the level of trust to a network node.

3.The base station performs steps 9,10 of the algorithm for determining the confidence level to the network node.

4. If a node has been successfully verified, the base station notes that the node is able to be the CH.

5. The base station sends a message to each node that the cluster head selection process is completed. Moreover, BS sends a message to each potential cluster head CH_temp that they can become the CH.

After BS has selected the potential cluster heads, the network clustering algorithm starts. The idea of the algorithm is that each temporary cluster head (CH_temp) must calculate the distance *d* between CH_temp and BS using formula (5). After that the CH_temp sends this *d* value along with the proposal to join the cluster to each neighboring nodes. Next, each node determines the minimal received value and acknowledges the appropriate CH_temp. In turn, each CH_temp compares its *d* value with the *d* values of the neighbors (CH_neighb) and if its value is the minimal, CH_temp proclaims itself the head of the cluster (CH) and notifies all its neighbors and the BS.

Network clustering algorithm

```
1: CHs_temp  calculate d
2: CHs_temp send Msg-Inv  to N_neighb.
3: Ni set CHs_temp  in the table of trusted nodes
4: for each N do
      Select $d_i$ = dmin
      Send msg to CH_temp with dmin
      end for
5: for CH_temp$_i$ do
      If di < dj
            then CH_temp$_i$ connect to CH_temp$_j$
      else CH_temp$_i$ = CH$_i$
      end for
6: CH$_i$ send  msg about CH  to CH_neighb. and BS
```

Node migration algorithm

Node migration algorithm. Since the nodes are mobile, often there will be a situation of node migration from cluster to cluster. New nodes in the network can appear, which will attempt to join the cluster. To resolve such situations there is a node migration algorithm. The algorithm represented in fig. 1 and works as follows.

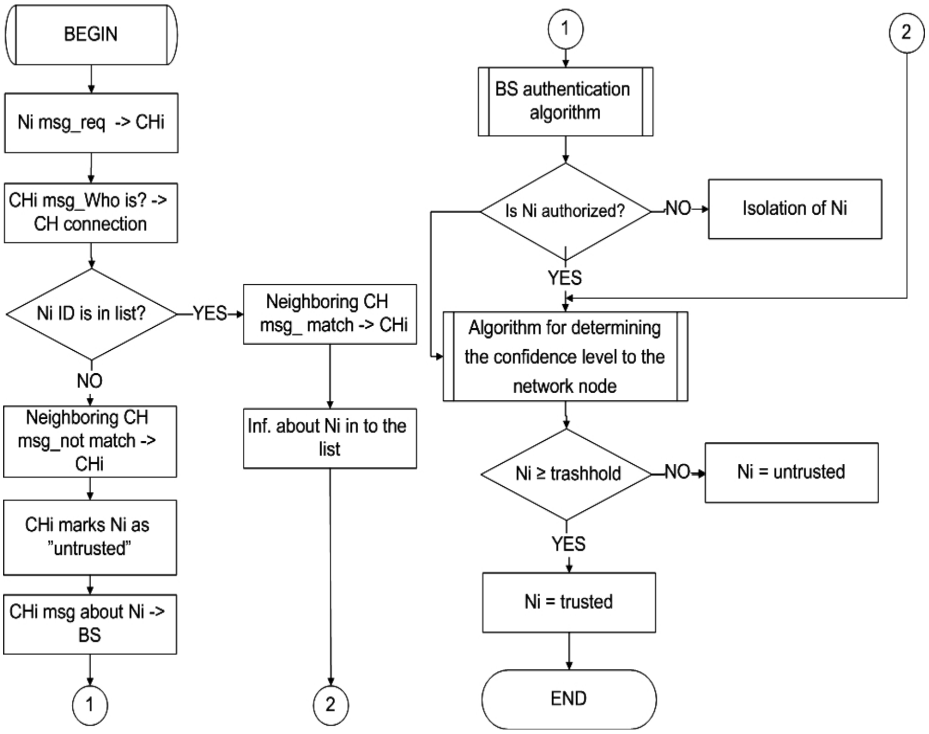
BEGIN
Ni msg_req -> CHi
CHi msg_Who is? -> CH connection
Ni ID is in list?
YES
NO
Neighboring CH msg_ match -> CHi
Inf. about Ni in to the list
Neighboring CH msg_not match -> CHi
CHi marks Ni as "untrusted"
CHi msg about Ni -> BS
1
2
1
BS authentication algorithm
Is Ni authorized?
NO
Isolation of Ni
YES
2
Algorithm for determining the confidence level to the network node
Ni ≥ trashhold
NO
Ni = untrusted
YES
Ni = trusted
END

Fig. 1. Node migration algorithm

To start this the cluster (CHi) has to determine whether a node that wants to join the cluster is new or previously existed. CHi sends a request to all neighboring cluster heads for the presence of a node in their tables. If the node is from a nearby cluster, CHi considers it is a trusted node and puts it in its own table. If it is a very new node, then CHi marks it as "untrusted" and conducts the authentication procedure. Next runs the algorithm for determining the confidence level to the network node (this procedure will be launched both for new node and for previously existed). After that node becomes either trusted or untrusted.

Conclusion. In this article a secure control protocol for mobile clustering wireless sensor network was submitted. Functioning of this protocol is described by set of algorithms that take into account the features of the mobile sensor network. This protocol with built-in algorithms of determining the confidence level and of trusted relationships between nodes allows to protect from the malicious insiders. In the future we plan to develop a network nodes authentication protocol based on lightweight cryptography that will protect the network from an external attacker and prevent the introduction of untrusted nodes in the network. Also we plan to make a network simulation to verify the effectiveness of the protocol.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Абрамов Е.С., Андреев А.В., Мордвин Д.В.* Применение графов атак для моделирования сетевых воздействий // Известия ЮФУ. Технические науки. – 2012. – № 1 (126). – С. 165-174.
2. *Kotenko, I.; Chechulin, A.* A Cyber Attack Modeling and Impact Assessment Framework // 5th International Conference on Cyber Conflict (CyCon), 2013. <http://ieeexplore.ieee.org/xpl/abstractReferences.jsp?arnumber=6568374> (28.02.2014).
3. *Ingols K., Lippmann R., Piwowarski K.* Practical attack graph generation for network defense // ACSAC. IEEE Computer Society. – 2006. – P. 121-130.
4. *Williams L., Lippmann R. and Ingols K.* GARNET: A graphical attack graph and reachability network evaluation tool // Visualization for Computer Security (VizSEC), ser. Lecture Notes in Computer Science, J.R. Goodall, G.J. Conti, and K.-L. Ma, Eds., vol. 5210. Springer, 2008. – P. 44-59.
5. Common Vulnerabilities and Exposures (CVE). <http://cve.mitre.org/> (28.02.2014).
6. *Mell P., Scarfone K., Romanosky S.* Common Vulnerability Scoring System (CVSS). <http://www.first.org/cvss/cvss-guide.html> (28.02.2014).
7. *Andreev A.V., Mordvin D.V., Abramov E.S., Makarevich O.B.* Corporate networks security evaluation based on attack graphs // Proceedings of the 4rd international conference on Security of information and networks (SIN '11). ACM, New York, NY, USA. – P. 29-36.
8. National Institute of Standards and Technology, "National Vulnerability Database, NVD. <http://nvd.nist. gov> (28.02.2014).
9. *Mordvin D.V., Abramov E.S., Makarevich O.B.* Automated method for constructing of network traffic filtering rules // Proceedings of the 3rd international conference on Security of information and networks (SIN '10). ACM, New York, NY, USA. – P. 203-211.
10. *Абрамов Е.С., Андреев А.В., Мордвин Д.В.* Методы автоматизации построения правил фильтрации сетевого трафика // Информационное противодействие угрозам терроризма. – 2010. – № 14. – С. 121-127.
11. *Абрамов Е.С., Андреев А.В., Мордвин Д.В.* Метод и алгоритмы построения правил разграничения доступа между узлами сети // Информационное противодействие угрозам терроризма. – 2010. – № 14. – С. 127-132.
12. Security and Privacy Controls for Federal Information Systems and Organizations // National Institute of Standards and Technology. <http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf> (28.02.2014).
13. *Anoop Singhal, Ximming Ou* NIST Interagency Report 7788 "Quantitative Security Risk Assessment of Enterprise Networks". <http://csrc.nist.gov/publications/nistir/ir7788/NISTIR-7788.pdf> (28.02.2014).

Статью рекомендовал к опубликованию к.т.н. М.Н. Казарин.

Абрамов Евгений Сергеевич – Южный федеральный университет; e-mail: abramoves@sfedu.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634371905; кафедра безопасности информационных технологий; зав. кафедрой.

Басан Елена Сергеевна – e-mail: ele-barannik@yandex.ru; кафедра безопасности информационных технологий; аспирантка.

Виджай Лакшми – Национальный технологический институт им. Малавия; e-mail: vlaxmi@mnit.ac.in; Джайпур, Индия; кафедра компьютерных технологий; профессор.

Abramov Evgeny Sergeevich – Southern Federal University; e-mail: abramoves@sfedu.ru; Block "I", 2, Chehov street, Taganrog, 347928, Russia; phone: +78634371905; the department of security in data processing technologies; head the department.

Basan Elena Sergeevna – e-mail: ele-barannik@yandex.ru; the department of security in data processing technologies; postgraduate student.

Vijay Laxmi – Malaviya National Institute of Technology; e-mail: vlaxmi@mnit.ac.in; Jaipur, India; the department of computer engineering; professor.