Secure Multipath Routing Algorithm with Optimal Balancing Message Fragments in MANET

Oleksandra S. Yeremenko, Ali Salem Ali

***Abstract*—This paper is devoted to the proposition of the algorithm of secure multipath routing with optimal balancing message fragments number in MANET. The work considered the concept of the threshold secret sharing scheme in relation to secure routing using non-overlapping paths for the message fragments transmission. Based on the analysis of disadvantages of existing mechanism SPREAD, it was proposed to improve the fragments allocation model, which had been reduced to the optimal balancing of message fragments number transmitted over the non-overlapping paths. Several optimality criteria were suggested as to the solution of balancing problem using Shamir`s scheme with or without redundancy. In the comparative analysis it was justified to use optimality criterion in practice, providing, on the one hand, minimization of dynamically managed upper bound number of fragments transmitted over separate non-overlapping paths in the network, and on the other hand – adaptation to security parameters (probability of compromise) of individual network elements: nodes, links and paths. Numerical examples of models with different optimality criteria of the solutions obtained, and their comparative analysis were presented. Within the proposed algorithm it is suggested to use the model under which the minimum number of fragments is transmitted by the worst path in terms of the probability of compromise, whereas their maximum number - by the best path.**

***Keywords*—Secure routing, MANET, probability of compromise, number of fragments balancing, non-overlapping paths.**

I. Introduction

MOBILE self-organizing networks MANET (Mobile Ad Hoc Network) is widely used nowadays in various applications as it was shown by the analysis. In accordance with the principles of its construction MANET is a complex organizational and technical system, which includes distributed in a certain area mobile nodes with the role of the structural and functional adaptation to signal interference situation, number and content of the supported services, requirements to Quality of Service and security level of transmitted data. Along with the objectives of guaranteeing Quality of Service in the MANET design and operation the key challenge is to ensure information security of the data transmitted by the network [1].

Compared to wired networks ensuring of information security in MANET is associated with the detection and prevention of many existing vulnerabilities and attacks [2]. Firstly, wireless channels are more susceptible to attacks such as passive listening (eavesdropping), active interference of signals and jamming. Secondly, the majority of routing protocols in MANET imply trusted interaction between participating nodes for packet transmission. Dependence on such interaction makes data more vulnerable to unauthorized access, data substitution, and attacks such as "Denial of Service" (DoS). Thirdly, the absence of fixed infrastructure and centralized management makes it difficult to apply many of the traditional solutions to ensure information security.

II. Threshold Message Sharing Mechanism

One of the approaches of ensuring the specified level of information security in communication networks is the implementation of SPREAD mechanism [3, 4], based on the multipath message routing after its fragmentation to parts in accordance with the Shamir`s scheme [3-5] (fig. 1). As a result of using SPREAD mechanism it is possible to reduce the probability of compromise of the transmitted message, because it complicates the adversary`s task: it must compromise not only one path that passed undivided message, but all paths transmitting its fragments. A message is compromised in case of unauthorized access to its content, i.e. in order to compromise the message, transmitted using SPREAD mechanism, all the paths used to deliver message fragments must be compromised. Thus, the fact of a compromised path is adversary access to all message fragments, transmitted over this path.

It should be noted that probability of compromise of individual path depends on the number of nodes and links it consists of and their security parameters, i.e. each element of the path (node, link) can be compromised with a certain probability. In general, various paths used to transmit the

Manuscript received March 12, 2015.

Oleksandra Yeremenko is with Kharkiv National University of Radio Electronics. Faculty of Telecommunications and Instrumentation, Department of Telecommunication Systems, Kharkiv, Ukraine (corresponding author to provide phone/fax: +38057-702-13-20; e-mail: alexere@ukr.net)

Ali Salem Ali is with Al Iraqi University, Network Engineering Department, Adhamiya, Baghdad, Iraq (e-mail: Alialbander2004@yahoo.com).

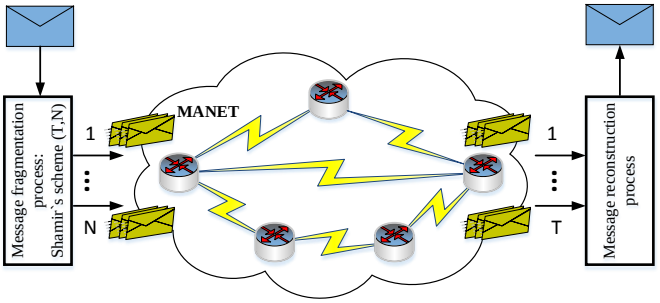

Fig. 1. Message fragmentation according to Shamir`s scheme.

message fragments obtained in accordance with the Shamir`s scheme [3-5] can have different values of the probability of compromise. Unfortunately, under the well-known mathematical models [3, 4] devoted to realization of SPREAD in message fragments allocation over the non-overlapping paths security parameters (such as the probability of compromise) of these are not taken into account explicitly. Thus, the actual problem seems related to the improvement of the mathematical model of secure routing message transmitted over the network based on the optimal allocation of its fragments over non-overlapping paths resulting from the use of applying Shamir`s scheme, and comprehensive address to the security parameters of available paths.

III. Secure Routing Models

Within the model let it be assumed that the following inputs are known:

- S_{msg} and D_{msg} – sender and receiver of a transmitted message;
- M – number of used non-overlapping paths in routing message fragments;
- (T, N) – Shamir`s scheme parameters, where $N$ – total number of fragments, obtained by applying the Shamir`s scheme; T – minimum number of fragments ($T \le N$) needed for the message reconstruction;
- p_i^j – probability of compromise j-th element (node, link) of i-th path;
- M_i – number of elements in the i-th path that can be compromised;
- γ_P – acceptable probability of compromise of message in the network.

In addition, the following parameters should be introduced in the model description:

- n_i – number of fragments, transmitted over the i-th path ($i = \overline{1, M}$);
- P_{msg} – probability of compromise for the whole message during its transmission by fragments over the network.

It is assumed that the sender and the receiver are trusted, i.e. probability of compromise of the sender and receiver nodes is equal to zero. Furthermore, within the proposed solution (as in [3-5]) it is supposed that if the element (node, link) is compromised, all fragments transmitted through the element will also be compromised. Then the probability of compromise of the i-th path consisting of the M_i elements can be calculated by the expression

$$p_i = 1-(1-p_i^1)(1-p_i^2)\dots(1-p_i^{M_i}) = 1-\prod_{j=1}^{M_i}(1-p_i^j). \quad (1)$$

Besides, during the calculation of the control variables n_i ($i = \overline{1, M}$) regulating the allocation of the message fragments over the non-overlapping paths the following condition [2-4] must be met:

$$N = \sum_{i=1}^{M} n_i . \quad (2)$$

In the case of Shamir`s scheme with redundancy when $T < N$ the condition below must be satisfied

$$N - n_i < T , (i = \overline{1, M}). \quad (3)$$

while when $T = N$ the following conditions must be met in the non-redundant sharing scheme

$$1 \le n_i \le T-1 , (i = \overline{1, M}). \quad (4)$$

Condition (4) ensures that in the case of compromising all the paths except i-th path an adversary cannot reconstruct the whole message.

One of the main conditions to be satisfied within the secure routing is that the probability of compromise of the message transmitted over the network must not exceed a specified acceptable value

$$P_{msg} \le \gamma_P . \quad (5)$$

For example, the probability of compromise of a message divided to the N fragments using Shamir`s scheme with parameters (N, N) transmitted over the M paths determined by the expression

$$P_{msg} = \prod_{i=1}^{M} p_i . \quad (6)$$

Satisfaction of condition (5) in accordance with expressions (1) and (6) must be provided during the pre-solution of the problem of calculation of the set of non-overlapping paths in the network. Model 1 may use expressions (1)-(6) proposed in works [3, 4]. Model 1 can be modified due to its disadvantages in relation to optimality of allocation message fragments over the transmission paths.

Model 2 includes constraint conditions (1), (2), (4)-(6) but uses as a criterion of optimal allocation fragments number over the non-overlapping paths the minimum of objective function

$$J = \sum_{i=1}^{M} p_i n_i , \quad (7),$$

which ensures secure routing over the network when the maximum number of message fragments will be sent over the path with the minimum probability of compromise. Conversely over the path with the highest probability of

compromise will be transmitted the minimum number of message fragments.

Model 3 can be described by the following terms. To ensure the optimal balancing of transmitted message fragments over multiple non-overlapping paths to the structure of improved model additional conditions are introduced:

$$n_i \le \beta \ \ (i = \overline{1, M}), \tag{8}$$

where β is a dynamically managed upper bound number of fragments transmitted over separate non-overlapping paths in the network.

Then, as a criterion for optimal solution for the allocation of the number of transmitted message fragments over non-overlapping paths it is reasonable to choose the minimum of the following objective function

$$J = \beta + \sum_{i=1}^{M} p_i n_i \ . \tag{9}$$

Minimization of equation (9) should be carried out under the conditions of constraint equations (2) and (8), thus reducing by the value β maximum number of fragments transmitted in each of the selected paths. Introduction to the object function (9) the term $\sum_{i=1}^{M} p_i n_i$ is aimed at achieving the following objective: if the total number of fragments N is not a multiple of paths number M, then the greater number of fragments will be transmitted over the best path in terms of the probability of compromise. This is the main advantage of the proposed solution and difference from the existing models [3-5].

Model 4 is represented by constraint conditions (1), (2), (5), (6), but the objective function below was chosen as optimality criterion

$$J = \sum_{i=1}^{M} (p_i n_i)^2 \ , \tag{10}$$

which is an extension of the expression (7).

IV. Comparative Analysis of Secure Routing Models

Comparative analysis of solving a problem of allocation message fragments over the non-overlapping paths of four models with different optimality criterions was performed.

Features of the models and proposed solutions (Model 1 ÷ Model 4) will be demonstrated by the following example. Suppose that a pair of nodes, a sender and a receiver, is given, and there are three non-overlapping paths available with different number of elements, nodes and links, between them (fig. 2). Within the example it is agreed that just links can be compromised, which is fair enough for MANET. For the purpose of calculations the following will be assumed:

- for the message fragmentation two cases of Shamir`s scheme are used: (10, 10) without redundancy, and (8, 10) with redundancy;
- the probability of compromise for communication links in accordance with their numbering and belonging to non-overlapping paths in MANET (fig. 2) takes the following values: $p_1^1 = 0{,}5$; $p_1^2 = 0{,}6$; $p_2^1 = 0{,}75$; $p_3^1 = 0{,}45$; $p_3^2 = 0{,}1$; $p_3^3 = 0{,}2$.

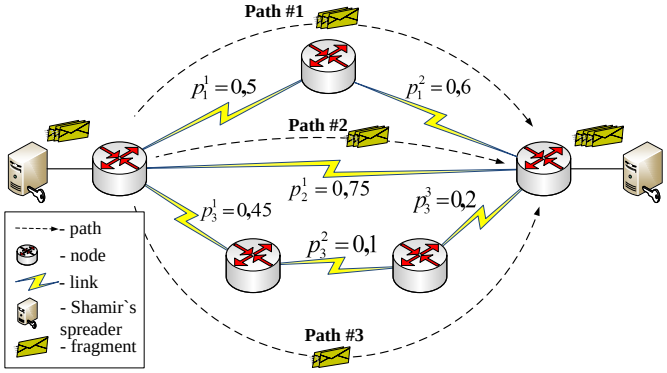

Fig. 2. Initial structure of MANET.

In accordance with expression (1) the following values of the probability of compromise for every path were calculated: $p_1 = 0{,}8$; $p_2 = 0{,}75$; $p_3 = 0{,}604$.

Table 1 shows the valid solutions of the problem of message fragments allocation over the non-overlapping paths obtained through the use of the previously described models.

Consider the case of using the Shamir`s scheme without redundancy, for example, (10, 10). the analysis of calculation results and the comparison of the obtained values of message fragments number allocated over the different paths showed that all four models can give satisfactory solutions. This can be explained by the fact that for compromising the whole message all three paths should be compromised. However, the best models are Model 3 and Model 4, since they imply adaptation to security parameters (Table 1), when the maximum number of message fragments is transmitted over the best path in terms of probability of compromise.

While using Model 1 (Table 1) one of the possible solutions of message fragments allocation over non-overlapping paths is when the maximum number of fragments ($n_1 = 8$)will be transmitted by the worst path in terms of probability of compromise ($p_1 = 0{,}8$), which is a disadvantage of this model.

TABLE I
Comparison of Existing Model and Improved Models of Message Fragments Allocation with Optimal Balancing

Model #	Number of message fragments in path depending on the allocation method			
	Model 1	Model 2	Model 3	Model 4
Path #	Shamir`s scheme (10, 10)			
1	8	1	2	3
2	1	1	4	3
3	1	8	4	4
Path #	Shamir`s scheme (8, 10)			
1	4	1	2	3
2	3	1	4	3
3	3	8	4	4

According to Model 2 using Shamir`s scheme (10, 10) message fragments allocation over the network paths showed

that the maximum number of fragments ($n_3 = 8$)passed over the best in terms of probability of compromise path ($p_3 = 0{,}604$), and their minimum number ($n_1 = 1$) was transmitted in the worst case ($p_1 = 0{,}8$).

Consider the case of using the Shamir`s scheme with redundancy, for example, (8, 10). The best solutions were provided by Model 1 and Model 4, because for compromising the whole message all three paths should be compromised. While in Model 2 the adversary needs to compromise just one path for the reconstruction of the transmitted message ($n_3 = 8$, $T = 8$), and in Model 3 two paths should be compromised ($n_2 = 4$, $n_3 = 4$, $T = 8$).

Model 1 with redundancy based on conditions (1)-(3), (5), (6 provides quite a good solution in terms of optimal allocation of message fragments over non-overlapping paths (Table 1). From the practical viewpoint it is desirable that the process of fragments allocation over the network paths must be balanced to make adversary`s tasks as complicated as possible.

Model 4, based on constraint conditions (1), (2), (5), (6) and the optimality criterion (10), gives the best solution compared to all four models. Using this model it is possible to provide on the one hand the optimal balancing of message fragments transmitted over separate non-overlapping paths in the network, and on the other hand – adaptation to security parameters (probability of compromise) of individual network elements: links and paths. In this case the minimum number of fragments ($n_1 = 3$) is transmitted by the worst path in terms of the probability of compromise, andtheir maximum number ($n_3 = 4$) is transmitted by the best one (Table 1). Therefore, the solution obtained by Model 4 is more preferable because of its ability to adapt to the security parameters of network paths.

V. Conclusion

Thus, the algorithm for secure multipath routing with optimal balancing message fragments in MANET includes the following steps:

1. Analysis of MANET architecture (number of network elements, Quality of Service and security requirements, signal-noise conditions etc).
2. Calculation of the set of non-overlapping paths between given sender and receiver nodes in consequence of condition (5).
3. Fragmentation of transmitted message according to selected Shamir`s scheme with or without redundancy.
4. Optimal allocation of the message fragments over the set of non-overlapping paths based on the model including expressions (1), (2), (5), (6) and optimality criterion (10).

Disadvantages of existing solutions consist in the fact that the process of allocation of message fragments over the non-overlapping paths is not balanced and doesn't provide adaptation of the obtained solutions to security parameters of network elements. Therefore, within the existing models [3-5] it may occur with the fragments allocation that the worst path in terms of the probability of compromise will transmit the maximum number of fragments. Nevertheless, the proposed model procedure for allocation of the transmitted message fragments over the non-overlapping paths is more adapted to security parameters (for example, the probability of compromise) of the individual network elements: nodes, links, and paths. This can be confirmed by the numerical results, when the minimum number of fragments is transmitted by the worst path in terms of the probability of compromise, and their the maximum number is passed by the best one.

The suggested algorithm may be used in practice within secure multipath routing with optimal balancing of message fragments transmitted over the non-overlapping paths. That is due to the fact that one of the key problems in operation of mobile self-organizing networks is ensuring of information security for data transmission through communicational links which in turn are the most vulnerable in MANET.

References

[1] *RFC 2501. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations*. 1999.

[2] *ITU-T X-805. Security architecture for systems providing end-to-end communications*. 2003.

[3] W. Lou, W. Liu, Y. Fang, "SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks", *INFOCOM 2004, Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE*, Vol. 4, 2004, pp. 2404-2413.

[4] W. Lou, Y. Kwon, "H-SPREAD: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks", *Vehicular Technology, IEEE Transactions on*, Vol. 55, Issue 4, 2006, pp. 1320-1330.

[5] S. Alouneh, A. En-Nouaary, A. Agarwal, "A Multiple LSPs Approach to Secure Data in MPLS Networks", *Journal of Networks*, Vol. 2, Issue 4, 2007, pp. 51-58.

Oleksandra S. Yeremenko received her Ph.D. in Telecommunication Systems and Networks from the Kharkiv National University of Radio Electronics (2008) and academic rank of Senior Researcher (2012). She joined the Department of Telecommunication Systems at the Kharkiv National University of Radio Electronics as a senior research assistant in 2007. She has been an associate professor of the Department of Telecommunication Systems since 2011. Her current research interests are NGN, TCP/IP, Network Security, and Fault-Tolerant Routing.

Ali Salem Ali received his B.Sc. in Computer Science from the Al-ma`amoon University, Baghdad, Iraq (2005) and M.Sc. from the National Technical University Kharkiv Polytechnic Institute (2008). He received his Ph.D. in Telecommunication Systems and Networks from the Kharkiv National University of Radio Electronics (2012). He joined the Network Engineering Department at the Al Iraqi University (Iraq, Baghdad, Adhamiya) as a Teacher in 2012. His current research interests are in the area of Network Protocols and Routing.