УДК 621.391.7 (043.2)

O.S. Yeremenko
Kharkiv National University of Radio Electronics, Kharkiv

METHOD OF OPTIMAL BALANCING OF MESSAGE FRAGMENTS NUMBER IN SECURE MULTIPATH ROUTING

One of the approaches of ensuring the specified level of information security in MANET (Mobile Ad Hoc Networks) is the implementation of SPREAD mechanism, based on the multipath message routing after its fragmentation to parts according to the Shamir`s scheme. Using SPREAD it is possible to reduce the probability of compromise of transmitted message, because it is not the only one path must be compromised, but all paths transmitting its fragments.

Within the model the following inputs are known: 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, next parameters in model introduced: 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.

Assumed that probability of compromise of sender and receiver is equal to zero. Furthermore, within the proposed solution 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 as

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

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 it must be met the following condition:

$$N = \sum_{i=1}^{M} n_i \,. \tag{2}$$

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

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

while in the non-redundant sharing scheme $T = N$ it takes the form

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

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

$$P_{msg} \le \gamma_P \,. \tag{5}$$

Probability of compromise of message divided to N fragments using Shamir`s scheme with parameters (N, N) transmitted over the M paths is

$$P_{msg} = \prod_{i=1}^{M} p_i \,. \tag{6}$$

As optimality criterion in proposed method is chosen the next objective function

$$J = \sum_{i=1}^{M} \left(p_i n_i \right)^2 \,. \tag{7}$$

Therefore, the method for secure multipath routing with optimal balancing message fragments in MANET includes the following steps: calculation of set of non-overlapping paths between given sender and receiver using condition (5); fragmentation of transmitted message according to selected Shamir`s scheme with or without redundancy; optimal allocation of the message fragments over the set of non-overlapping paths based on the model (1), (2), (5), (6) and optimality criterion (7).

Within the existing models it is possible the situation of fragments allocation when the worst in terms of the probability of compromise path will transmit maximum number of fragments. While in accordance with the proposed method allocation of message fragments over the non-overlapping paths is more adapted to security parameters (probability of compromise) of the individual network elements: nodes, links, and paths, that was confirmed by the numerical results.