УДК 519.676

СИНТЕЗ СХЕМ ПРЕДВАРИТЕЛЬНОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ С ИСПОЛЬЗОВАНИЕМ ВЗАИМНО ДОПОЛНЯЮЩИХ УСЛОВИЙ ИХ КОРРЕКТНОСТИ

А.В. Затей

На основе вероятностных оценок и компьютерных экспериментов с применением вероятностных алгоритмов синтеза схем предварительного распределения ключей в компьютерной сети показано, что сочетанием условий корректности двух известных таких схем (KDP, Key Distribution Pattern и HARPS, Hashed Random Preloaded Subset Key Distribution) возможно повышение информационной скорости комбинированной схемы (HAKDP, Hashed Key Distribution Pattern) по сравнению с информационной скоростью этих схем.

Ключевые слова: компьютерная сеть, системный ключ, предварительное распределение ключей, информационная скорость.

ВВЕДЕНИЕ

Схемы предварительного распределения ключей в компьютерной сети предусматривают формирование доверенным центром на основе исходной секретной системной ключевой информации пакетов одинаковых по объему секретных единиц ключевой информации для каждого участника сети и пересылка этих пакетов соответствующим участникам. При этом состав этих пакетов и, возможно, некоторая дополнительная несекретная информация о них публикуется на общедоступном сервере. Полученная каждым участником секретная ключевая информация должна быть достаточной для вычисления каждым из них рабочих ключей для связи с участниками той или иной группы из числа групп, в которые он входит и состав пакетов секретной информации которых ему известен. Состав самих групп также общеизвестен и публикуется. Такие группы называются привилегированными. С другой стороны, имеются так называемые отчужденные группы участников. В правильно построенной схеме участники такой группы на основе объединения полученных каждым из ее участников пакетов секретной информации не должны быть в состоянии вычислить рабочий ключ никакой привилегированной группы. Это гарантируется *условием корректности* схемы.

Схемы предварительного распределения ключей характеризуются информационной скоростью – величиной, обратной к суммарной длине секретных пакетов, направляемых участникам сети.

Чем меньше секретной информации передаётся по закрытым каналам, тем больше информационная скорость. Информационная скорость схемы – основной параметр ее эффективности, чем она больше, тем эффективнее схема.

Существует множество подходов к предварительному распределению. R. Blom и D. Stinson [1, 2, 3, 4] предложили алгебраические методы. P. Erdös [5, 6] изучал так называемые схемы предварительного распределения ключей, то есть, семейства подмножеств с парными или в более общем случае r-мерными пересечениями, являющимися семействами Шпернера. Вероятностные алгоритмы для синтеза схем KDP (Key Distribution Pattern) были предложены в [7]. Все эти методы исключительно безопасны. В статьях [8, 9, 10, 11, 12] было предложено несколько эффективных методов для предварительного распределения. Благодаря существенному снижению объема распределяемой секретной информации эти методы наиболее подходят для сетей мобильных устройств.

В настоящей работе показана возможность построения схем предварительного распределения ключей с условием корректности, являющимся дизъюнкцией условий корректности двух других схем как взаимно дополняющих: новая схема корректна, если она удовлетворяет хотя бы одному из этих условий. При этом с использованием вероятностных оценок и компьютерных экспериментов на основе вероятностных алгоритмов синтеза схем показана возможность повышения информационной скорости схемы предварительного распределения ключей с комбинированным условием корректности.

СХЕМЫ ПРЕДВАРИТЕЛЬНОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ С ХЕШИРОВАНИЕМ

В настоящей работе изучаются схемы предварительного распределения *q* системных ключей с хешированием *HAKDP*(***P***,***F***,*L*)(*n,q*) (Hashed Key Distribution Pattern) в компьютерной сети из *n* абонентов, в которых допускаются коалиции *F* участников из множества **F** "отчужденных" коалиций и группы *P* участников из множества **P** привилегированных групп участников. Ниже будем интерпретировать такие коалиции и группы как множества номеров входящих в них абонентов сети – подмножества множества **U**={1,2,..,*n*}. Для получения такой схемы из исходного множества **K**, |**K**|=*q*, системных ключей (двоичных наборов фиксированной длины) образуется *n* подмножеств K_i, *i*=1,...,*n*, *системных ключей, назначаемых i*-му участнику. Для каждого участника определяется и публикуется на сервере пара числовых наборов (S_i, D_i). Наборы S_i содержат номера системных ключей из подмножеств K_i , а наборы D_i содержат числа D_i (s), $0 \le D_i \le L$, применений к этим ключам криптографической бесключевой хеш-функции h:$\{0,1\}^k \to \{0,1\}^k$. Получаемые в результате возможно многократного применения к системному ключу хеш-функции образы системных ключей передаются *i*-му участнику по закрытому каналу.

Информационная скорость схемы предварительного распределения ключей при этом определяется как величина $\rho = 1/\sum_{i=1}^{n}|K_i|$, обратная суммарному количеству образов системных ключей, пересылаемых по закрытым каналам [3].

Для вычисления общего ключа привилегированной группы *P* каждый её участник (*i*-й абонент сети) должен применить функцию хеширования к полученному образу s-го системного ключа $\max_{j\in P} D_j(s) - D_i(s)$ раз.

Рабочий ключ, вычисляемый каждым участником группы *P* по образам системных ключей с номерами из множества $\bigcap_{i\in P} S_i$, имеющихся у каждого такого участника, не должен вычисляться участниками отчужденной группы на основе объединения полученных ими образов системных ключей, т. е. по образам ключей из множества $\bigcup_{i\in F} S_i$.

Таким образом, указанные числовые наборы должны соответствовать предикату:

$$\forall P \in \mathbf{P}, F \in \mathbf{F}, P \bigcap F = \varnothing : \bigcap_{i\in P} S_i \neq \varnothing \wedge \\ \wedge \neg\{[\bigcap_{i\in P} S_i \subseteq \bigcup_{j\in F} S_j] \wedge \\ \wedge [\forall s \in \bigcap_{i\in P} S_i \max_{i\in P} D_i(s) \geq \min_{j\in F} D_j(s)]\}. \quad (1)$$

Тогда, если применяется криптографическая хеш-функция, участники никакой "отчужденной" коалиции не могут вычислить общий ключ участников никакой привилегированной коалиции.

Изучаемые в работе *HAKDP*(**P**,**F**,*L*)(*n,q*)-схемы, с одной стороны, являются обобщением *KDP*(**P**,**F**)(*n,q*)-схем (Key Distribution Pattern) [1–4], в которых не применяется хеширование, и которые описываются наборами множеств S_i номеров системных ключей, соответствующих предикату:

$$\forall P \in \mathbf{P}, F \in \mathbf{F}, P \bigcap F = \varnothing : \bigcap_{i\in P} S_i \neq \varnothing \wedge \\ \wedge \neg[\bigcap_{i\in P} S_i \subseteq \bigcup_{j\in F} S_j] \quad (2)$$

с другой стороны, они являются специальным подклассом так называемых *HARPS*(*n,q*)-схем (*HARPS* – Hashed Random Preloaded Subset Key Distribution) [6], в которых каждому участнику доставляются все системные ключи из множества **K** ($\forall i \in P \bigcup F : S_i = \{1,...,q\}$) и предикат соответствия имеет более простой вид:

$$\forall P \in \mathrm{P}, F \in \mathrm{F} : P \bigcap F = \varnothing \wedge \\ \wedge \neg\{[\forall s \max_{i\in P} D_i(s) \geq \min_{j\in F} D_j(s)] \quad (3)$$

Схемы, соответствующие предикату (2) впервые были описаны в работе [13]. В этой работе, как и в работе [7] они называются системами пересекающихся множеств (set intersection systems).

Неформальное пояснение понятия *HAKDP*(**P**,**F**,*L*)(*n,q*)-схемы, представленное в [14] формализуем следующим определением.

Определение [15]. HAKDP(**P**,**F**,*L*)(*n,q*)-*схемой, где* **P** *и* **F** *– это семейства подмножеств множества* **U** = {1, …, *n*}, *называется пара* ($\tilde{\mathbf{K}}$,**D**) *семейств* $\tilde{\mathbf{K}}$={$K_1,\ldots,K_n$} *подмножеств конечного множества* **K** *из q элементов* (*системных ключей*) *и* **D**={$D_1,\ldots,D_n$} *подмножеств множества* {0,1,…,*L*}, *причем* $|D_i| = |K_i|$ *и элементы множеств* D_i *взаимно однозначно соответствуют элементам множеств* K_i, *i*=1,…,*n*, *удовлетворяющая условию* (1) где S_i (*или* S_j) *наборы номеров элементов множества* **K,** *образующих множество* K_i (*или* K_j).

Представленные в этой формуле условия корректности HAKDP(**P,F**,*L*)(*n,q*)-схемы

1) $[\bigcap_{i\in P} S_i \not\subseteq \cup_{j\in F} S_j]$,

2) $[\exists s \in \bigcap_{j\in P} S_j : \max_{j\in P} D_j(s) < \min_{i\in F} D_i(s)]$

в (1) являются взаимно дополняющими: для корректности схемы (соответствия предикату (1)): достаточно выполнение хотя бы одного их них. Ниже будем называть первое из них KDP-условием, а второе – HA-условием. Этим обуславливается возможность сокращения как числа q=|**K**| распределяемых системных ключей, так и количества системных ключей, пересылаемых от доверенного центра участникам сети по защищенным каналам, то есть повышения информационной скорости системы предварительного распределения ключей.

Для синтеза схем предварительного распределения ключей наряду с детерминированными алгоритмами применяют вероятностные алгоритмы.

Так вероятностный метод синтеза *KDP* (**P,F,***n,q*)-схем впервые был описан в работе [7].

В настоящей статье обоснован вероятностный алгоритм синтеза *HAKDP*(**P**,**F**,*L*)(*n,q*)-схем с предварительной оценкой недостаточного и достаточного для его успешного завершения объемов q_0 и q ключевой информации – чисел системных ключей в исходном множестве **K**.

Входом алгоритма являются числа $0,5 \le p \le 1, L, 0 \le L, L \in Z$, а также множества **P** и **F** привилегированных групп участников и отчуждённых коалиций F участников. Выходом – указанная в определении пара семейств, вычисленная с использованием рандомизированных процедур выбора множеств K_i, i = 1, ..., n. При вероятностном формировании каждого множества K_i каждый элемент множества **K** включается в него с вероятностью p, а при формировании каждого множества Di его элементы выбираются из множества {0,…,L} с равными вероятностями 1\(L+1). Выбранная таким образом пара семейств ($\tilde{K}$**,D**) проверяется на соответствие предикату (1). При положительном результате верификации она возвращается, а при отрицательном формируется сообщение о неуспехе генерации схемы. Естественным расширением данного алгоритма является его использование в цикле с повторением цикла при неуспехе.

Положим $c=npq$ среднее значение $\sum_1^n K_i$ и $\rho=1/c$ – среднее значение информационной скорости HAKDP(**P,F**,*L*)(*n,q*)-схем, синтезируемых вероятностным методом.

Заметим, что при p=1 синтезированная алгоритмом схема не будет соответствовать KDP-условию (т.е. предикату (2)), а семейство **D** будет HARPS(**P,F**,*L*)(*n,q*)-схемой, при L=0 она не будет соответствовать HA-условию (т.е. предикату (3)), а семейство $\tilde{K}$ будет KDP(**P,F**)(*n,q*)-схемой. При других сочетаниях значений этих параметров, для успешного синтеза схемы достаточно соответствие тому или другому из этих условий (предикатов). В связи с этим и появляется возможность повышения информационной скорости схемы предварительного распределения ключей.

ОЦЕНКИ ОБЪЕМА КЛЮЧЕВОЙ ИНФОРМАЦИИ ДОСТАТОЧНОГО ДЛЯ УСПЕШНОГО СИНТЕЗА СХЕМЫ

По определению, паре ($\tilde{\mathbf{K}}$**,D**) взаимно однозначно соответствует пара семейств (**S,D**), где **S**={S_1,… ,S_n}. Если мощности элементов множества **P** равны g, а мощности элементов множества **F** равны w, то HAKDP(**P**,**F**,*L*)(*n,k*)-схему будем обозначать HAKDP(*g,w*,*L*)(*n,k*).

Ясно, что имеется некоторое значение q, при котором HAKDP(**P**,**F**,*L*)(*n,q*)-схема существует, а при меньшем значении |**K**|<q не существует. Практически найти эту точную нижнюю оценку и тем более построить схему не представляется возможным. В то же время при синтезе можно использовать верхнюю оценку для q. Ее можно получить, полагая, что все элементы множества **P** содержат одинаковые количества элементов g (минимальная мощность элемента из этого множества). Аналогично элементы множества **F** содержат одинаковые количества элементов w (максимальная мощность элемента из этого множества). Далее, при вычислении верхней оценки мы полагаем, что неравенство в формуле (1) из определения должно выполняться не для некоторого элемента, а для всех элементов. То есть верхнюю оценку будем рассчитывать исходя из соответствия предикату

$$\forall P \in \mathrm{P}, F \in \mathrm{F}, P \cap F = \varnothing : \bigcap_{i\in P} S_i \neq \varnothing \wedge \{[\bigcap_{i\in P} S_i \not\subseteq \cup_{j\in F} S_j] \vee \vee [\forall s \in \bigcap_{j\in P} S_j : \max_{j\in P} D_j(s) < \min_{i\in F} D_i(s)]\} \quad (4)$$

Пусть **P** – это семейство всех подмножеств множества **U** мощности g, **F** – семейство всех подмножеств множества **U** мощности w, причем $g+w \le n$.

Число $q=|\mathbf{K}|$ ключей, где E – вероятность успешного синтеза схемы за одну итерацию алгоритма, является достаточным для удачного синтеза схемы:

$$q < \frac{\log\left((1-\mathrm{E})\cdot\frac{g!w!}{(n-g-w+1)\cdot\ldots\cdot n}\right)}{\log\left(1-\left(p^{g}((1-p)^{w}+p^{w}\sum_{i=0}^{L}w^{-1}\frac{1}{L+1}\left(\frac{L-t}{L+1}\right)^{g+w+1})\right)\right)} \quad (5).$$

Ясно, что при меньшем, чем q количестве q' исходных системных ключей потребуется большее количество итераций вероятностного алгоритма для синтеза схемы.

КОМПЬЮТЕРНЫЕ ЭКСПЕРИМЕНТЫ И ВЫВОДЫ

Целью данного раздела является экспериментальное подтверждение полученных выше оценок и положительного эффекта использования в вероятностном алгоритме двух взаимно дополняющих условий корректности схемы, описанных выше.

Зафиксируем параметры n (количество участников сети) и $E = 0.5$.

Рассмотрим результаты расчета оценок и компьютерных экспериментов для двух серий схем

1) HAKDP(3, w, 20)(16,q), $w = 2,3$ и

2) HAKDP(3, w, 0)(16, q), $w = 2,3$

при варьируемых параметрах p вероятностного алгоритма. Схемы второй серии соответствуют предикату (3), при $p = 1$ схемы первой серии соответствуют предикату (2), при $p < 1$ они соответствуют предикату (2) или предикату (3), т.е., по совокупности – предикату (1) .

В таблице 1 для схем первой серии представлены значения q, полученные по формуле (5), q' – значение, которое удалось достигнуть экспериментально, в допустимые сроки по времени t<100 секунд. В таблице 2 представлены аналогичные результаты для экспериментов второй серии.

Данные таблицы показывают, что полученные аналитически оценки подтверждаются на практике, а именно, мы можем строить схемы с исходным количеством используемых системных ключей, меньшим, чем достаточное для построения схемы за одну итерацию вероятностного алгоритма количество q. При этом видно, что использование HA-условия в дополнение к KDP-условию влечет уменьшение достаточного q и экспериментально достигнутого q' исходного количества системных ключей.

В таблице 3 для схем первой и второй серий представлены $c'=pnq'$ – математические ожидания исходных количеств используемых системных ключей, образы которых направляются абонентам по закрытым каналам по схеме, синтезированной вероятностным алгоритмом с использованием параметра q'.

Таблица 1 – Результаты синтеза для набора параметров первой серии

p	w			
	2		3	
	q	q'	q	q'
0,5	289	145	609	290
0,6	226	110	541	*230*
0,7	196	94	503	210
0,8	178	*80*	447	205
0,9	160	76	357	205
0,95	148	75	308	205
0,99	134	75	274	205
1	130	75	266	205

Таблица 2 – Результаты синтеза для набора параметров второй серии.

p	w			
	2		3	
	q	q'	q	q'
0,5	365	235	768	640
0,6	331	220	868	720
0,7	370	240	1295	1010
0,8	556	325	2927	2350
0,9	1562	790	16440	–
0,95	5309	2560	111800	–
0,99	117300	–	–	–
1	–	–	–	–

Таблица 3 – Математические ожидания количеств используемых системных ключей для серий экспериментов.

p	w			
	2		3	
	c', $(L=20)$	c', $(L=0)$	c', $(L=20)$	c', $(L=0)$
0,5	1160	*1880*	2320	*5120*
0,6	1056	2112	*2208*	6912
0,7	1053	2688	2352	11312
0,8	*1024*	4160	2624	30080
0,9	1095	11376	2952	–
0,95	1140	38912	3116	–
0,99	1188	–	3247	–
1	1200	–	3280	–

В таблице 4 представлены суммарные количества c' системных ключей, выбранных вероятностным алгоритмом синтеза HAKDP(g,w,n,q)-схем из исходного их количества q' для формирования их образов, направляемых абонентам по закрытым каналам, при успешном завершении компьютерных экспериментов по синтезу схем указанных двух серий.

Данные таблицы 4 соответствуют расчетным данным таблицы 3: реальное число

единиц отличается от ожидаемого не более, чем на десятки единиц. Данные в нижних строках совпадают, т. к. в соответствующих схемах каждому абоненту назначаются все *q'* единиц исходной ключевой информации.

Таблица 4 – Значения количеств используемых системных ключей при успешном завершении синтеза схем.

p	*w*			
	2		3	
	c', *(L=20)*	*c',* *(L=0)*	*c',* *(L=20)*	*c',* *(L=0)*
0,5	1199	*1917*	2372	*5076*
0,6	1077	2100	*2198*	6809
0,7	1058	2654	2334	11306
0,8	*1028*	4153	2662	22519
0,9	1103	11299	2969	–
0,95	1120	38835	3135	–
0,99	1143	–	3245	–
1	1200	–	3280	–

Сравнение данных, выделенных курсивом в столбцах для первой серии схем (*L*=20), с данными в нижней строке показывает положительный эффект (повышения информационной скорости) использования KDP-критерия (в дополнение к HA-критерию). Сравнение выделенных курсивом данных в соседних столбцах для первой (*L*=20) и второй (*L*=0) серий схем показывает положительный эффект использования HA-критерия (в дополнение с KDP-критерию).

В данной работе получены и подтверждены компьютерными экспериментами оценки *q*, количеств f системных ключей, образы которых распределяются абонентам сети, достаточных для синтеза схемы за практически приемлемое число итераций вероятностного алгоритма синтеза HAKDP(*P,F,L*)(*n,q*)-схем. С использованием этих оценок и вероятностного алгоритма синтеза таких схем подтверждён положительных эффект использования двух взаимно дополняющих условий их корректности, выражающийся в повышении информационной скорости схемы, синтезированной вероятностным алгоритмом и удовлетворяющей хотя бы одному условию, относительно информационной скорости схем, синтезированных вероятностным алгоритмом по соответствию конкретному из этих условий.

Работа выполнена при финансовой поддержке РФФИ, проект №14-01-00671а.

СПИСОК ЛИТЕРАТУРЫ

1. Blom, R. Nopublic key distribution / R. Blom // Advances in Cryptology. Proceedinge of EURUCRYPT'82. Plenum. New York. – 1983. – P. 231–236.

2. Blom, R. An optimal Class of Symmetric key Generation Systems / R. Blom // Advances in Cryptology: Proc. of Eurocrypt 84, Lecture notes in Computer Science, 209, Springer-Verlag. – 1984. – P. 335–338.

3. Stinson, D. R. On Some Methods for Unconditionally Secure Key. Distribution and Broadcast Encryption / D. R. Stinson // Designs, Codes and Cryptography, Kluwer Academic Publishers, Norwell, MA, USA, 1997.

4. Stinson, D. R. Cryptography: Theory and practice / D. R. Stinson // Third Edition, CRC Press, Boca Raton, Florida, 2006.

5. Erdös, P. Families of Finite Sets in which no Set is Covered by the Unuon of 2 Others / P. Erdös, P. Francl, Z. Füredi // Journal of Combinatorial Theory. Series A. – 1982. – Vol. 33. P. 158–166.

6. Erdös, P. Families of Finite Sets in which no Set is Covered by the Unuon of r Others / P. Erdös, P. Francl, Z. Füredi // Israel Journal of Mathematics. – 1985. – Vol. 51. – P. 79–89.

7. Dyer, M. On key storage in secure networks / M. Dyer, T. Fenner, A. Frieze, A. Thomason // Journal of Cryptology. – 1995. – Vol. 8. – P. 189–200.

8. Ramkumar M. Pre-Loaded Key Based Multicast and Broadcast Authentication in Mobile ad-Hoc Networks. / M. Ramkumar, N. Memon, R. Simha // Globecom-2003.

9. Leighton, L. Secret-Key Agreement with out Public-Key Cryptography / L. Leighton, S. Micali // Advances in Cryptology-CRYPTO-1993. – 1994. P. 456–478.

10. Ramkumar, M. An efficient key predistribution scheme for ad hoc network security / M. Ramkumar, N. Memon // Selected Areas in Communications, IEEE Journal on. – 2005. – Vol. 23, Issue 3. – P. 611–621.

11. Ramkumar, M. Broadcast Encryption Using Probablistic Key Distribution and Applications / M. Ramkumar // Journal of Computers. – 2006. – Vol. 1, № 3. – P. 1–12.

12. Ramkumar, M. I-HARPS: an Efficient Key Pre-Distribution Scheme / M. Ramkumar // E-print Archive, Rep 138. – 2005. – P. 1–13.

13. Mitchell, C. J. Key storage in secure networks / C. J. Mitchell, F. C. Piper // Discrete Applied Mathematics. – 1988. – Vol. 21. – P. 215–228.

14. Frolov, A. B. Non-Centralized Key Pre-Distribution in Computer Networks / A. B. Frolov, I. I. Shchurov // IEEE Proceedings of International Conference on Dependability of Computer Systems DepCos-RELCOMEX 2008, Szklarska Poreba, Poland, Computer Society Conference Publishing Services. Los Alamitos, California, Washington, Tokyo, 2008, P. 179–188.

15. Фролов, А. Б. Схемы предварительного распределения ключей допускающие коалиции / А. Б. Фролов, А. В. Затей // Вестник МЭИ. – 2013. – № 6. – С. 166–172.

16. Щуров, И. И. Минимизация ключевого материала для построения безопасной сети / И. И. Щуров // Вестник МЭИ, Москва, Издательство МЭИ. – 2006. – № 6. – С. 112–118.

***Затей А.В**. – аспирант кафедры математического моделирования Национального исследовательского университета МЭИ, тел. +79166838541, e-mail: zateyav@mpei.ru.*